(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
20. Juni 2019 (20.06.2019)

W I P O | P C T

(10) Internationale Veröffentlichungsnummer
WO 2019/115580 Al

(51) Internationale Patentklassifikation:
H04L 29/08 (2006.01) *G06F 21/60* (2013.01)

(21) Internationales Aktenzeichen: PCT/EP20 18/084465

(22) Internationales Anmeldedatum:
12. Dezember 2018 (12. 12.2018)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2017 129 947.5
14. Dezember 2017 (14. 12.2017) DE

(71) Anmelder: **INNOGY INNOVATION GMBH** [DE/DE]; Lysegang 11, 45139 Essen (DE).

(72) Erfinder: **STÖCKER, Carsten;** Verdistraße 5, 40724 Hil¬den (DE).

(74) Anwalt: **COHAUSZ & FLORACK PATENT- UND RECHTSANWÄLTE PARTNERSCHAFTSGESEL¬LSCHAFT MBB, HENDRIK BÜCKER;** Bleichstraße 14, 4021 1 Düsseldorf (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,

WO 2019/115580 A1

(54) **Title:** METHOD FOR OPERATING A DECENTRALIZED STORAGE SYSTEM

(54) **Bezeichnung:** VERFAHREN ZUM BETREIBEN EINES DEZENTRAT..EN SPEICHERSYSTEMS

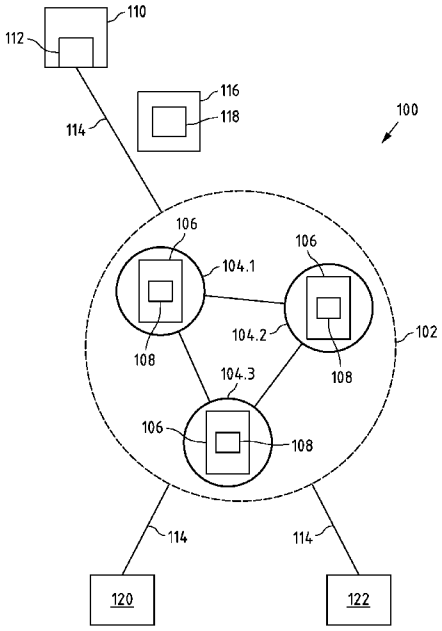

Fig.1

(57) Abstract: The invention relates to a method for operating a decentralized storage system (100, 500, 700) having at least one peer-to-peer network (102, 502, 702) having at least one peer-to-peer application (106, 506, 606), the method comprising: receiving, by means of the peer-to-peer application (106, 506, 606), at least one data set (116, 516), which comprises storage information (118, 518), from a data source (110, 510.1, 510.2, 510.3, 710); and executing a storage con¬trol means (108, 508, 608) of the peer-to-peer application (106, 506, 606) by means of at least some of the peer computers (104.1, 104.2, 104.3, 504, 702.1, 710.1) of the peer-to-peer network (102, 502, 702) in such a way that, on the basis of the storage information (118, 518) of the data set (116, 516) and a speci-fied storage comparison criterion, at least one storage assembly (120, 122, 520.1, 520.2, 520.3, 520.4) in which the data set (116, 516) will be stored is determined from at least two available different storage assemblies (120, 122, 520.1, 520.2, 520.3, 520.4) by means of the storage control means (108, 508, 608).

(57) Zusammenfassung: Die Anmeldung betrifft ein Verfahren zum Betrei¬ben eines dezentralen Speichersystems (100, 500, 700) mit mindestens einem Peer-to-Peer Netzwerk (102, 502, 702) mit mindestens einer Peer-to-Peer An¬wendung (106, 506, 606), wobei das Verfahren umfasst Empfangen, durch die Peer-to-Peer Anwendung (106, 506, 606), mindestens eines Datensatzes (116, 516), der eine Speicherungsinformation (118, 518) umfasst, von einer Daten¬quelle (110, 510.1, 510.2, 510.3, 710), und Ausführen eines Speicherungssteuer¬mittels (108, 508, 608) der Peer-to-Peer Anwendung (106, 506, 606) durch min¬destens einem Teil der Peer-Computer (104.1, 104.2, 104.3, 504, 702.1, 710.1) des Peer-to-Peer-Netzwerks (102, 502, 702), derart, dass basierend auf der Spei¬cherungsinformation (118, 518) des Datensatzes (116, 516) und einem vorge¬gebenen Speicherungsvergleichskriteriums mindestens eine Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4), in der der Datensatz (116, 516) gespei¬chert werden wird, aus

[Fortsetzung auf der nächsten Seite]

SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

zumindest zwei verfügbaren unterschiedlichen Speicheranordnungen (120, 122, 520.1, 520.2, 520.3, 520.4) durch das Speicherungssteuermittel (108, 508, 608) bestimmt wird.

Verfahren zum Betreiben eines dezentralen Speichersystems

Die Anmeldung betrifft ein Verfahren zum Betreiben eines dezentralen Speichersystems. Darüber hinaus betrifft die Anmeldung ein dezentrales Speichersystem und eine Peer-to-Peer-Anwendung.

Bei Offshore-Windparks, aber auch bei anderen Anwendungen (z.B. Fahrzeugen, Drohnen, Wetter Stationen, Smart Meter, Wearables, Smartphones, Überwachungskameras, Medizinischen Geräten, u.a. oder allgemeiner ‚Internet der Dinge' Geräten), wird eine Vielzahl von Daten erfasst. So weist eine Windkraftanlage eine Vielzahl von Sensoren auf, die Daten nahezu kontinuierlich erfassen. Hierbei kann die Windkraftanlage als eine Datenquelle mit einer Mehrzahl von unterschiedlichen weiteren Datenquellen (z.B. Sub-Datenquellen) angesehen werden. Die mindestens eine Datenquelle überträgt die erfassten Daten (z.B. gemessene Temperaturwerte, gemessene elektrische Strom-, Spannungs- oder Leistungswerte, gemessene Umdrehungswerte, gemessene Druckwerte, gemessene Windgeschwindigkeiten, gemessene Stillstandszeiten, gemessene Vibrationen etc.) in Form von einem oder mehreren Datensatz/sätze an eine zentrale Steuerung des Offshore-Windparks.

Die zentrale Steuerung des Offshore-Windparks in Form eines oder mehrerer Server/s weist in der Regel zwei oder mehr unterschiedliche Speicheranordnungen bzw. Datenbanken auf. Die Speicheranordnungen können sich insbesondere hinsichtlich ihrer Speichersicherheit unterscheiden. Mit anderen Worten können die mindestens zwei Speicheranordnungen jeweils einen unterschiedlichen Speichersicherheitslevel haben bzw. bereitstellen. Beispielsweise kann eine erste Speicheranordnung einen ersten Speichersicherheitslevel, der insbesondere eine (im Wesentlichen) revisionssichere Speicherung von Datensätzen erlaubt. Dies ist in der Regel mit einem hohen Aufwand verbunden. Daher ist in der Regel mindestens eine

weitere Speicheranordnung (z.B. eine Cloud) vorgesehen, die im Vergleich zu der ersten Speicheranordnung eine geringere Speichersicherheit bzw. einen geringeren Speichersicherheitslevel bereitstellt. Bei einer solchen Speicheranordnung ist jedoch auch im Vergleich zu der ersten Speicheranordnung der Aufwand für die Bereitstellung der Sicherheit geringer. Für eine effiziente Speicherung von einer Vielzahl von Datensätzen ist es daher ein stetiges Anliegen, nur die Datensätze in der ersten Speicheranordnung zu speichern, für die tatsächlich ein hoher Speichersicherheitslevel erforderlich ist.

Gemäß dem Stand der Technik wird hierzu vorab definiert, welche Datensätze einen hohen (Speicher-)Wert aufweisen und damit in der ersten Speicheranordnung gespeichert werden sollten, und welche Datensätze einen geringeren Wert aufweisen und damit in der mindestens einen weiteren Speicheranordnung gespeichert werden sollten. Die zentrale Steuerung ist hierbei eingerichtet, für einen empfangenen Datensatz entsprechend der vorab definierten Kriterien die Speicheranordnung aus den mindestens zwei Speicheranordnungen zu bestimmen bzw. auszuwählen, in der der empfangene Datensatz gespeichert werden wird.

Bei dieser bekannten Speicherungssteuerung stellt die zentrale Steuerung bereits ein Sicherheitsrisiko dar. So besteht bei einer derartigen Server-Client-Struktur neben den hohen Transaktionskosten, die durch eine entsprechende Architektur entstehen, der Nachteil, dass die zentrale Steuerinstanz bzw. der zentrale Steuerserver vertrauliche Daten (definierte Kriterien für die Speicherung von Datensätzen und temporär die Datensätze) aufweist und vertrauliche Datensätze verarbeitet. Ein ständiges Problem der zentralen Steuerung bzw. zentralen Steuerungsinstanz ist, die auf einem oder mehreren Server/n gespeicherten bzw. zu verarbeiteten vertraulichen Daten vor einem Zugriff eines unberechtigten Dritten zu schützen. lnsbesondere ist ein großer sicherheitstechnischer Aufwand erforderlich, um eine Manipulation beispielsweise der definierten Kriterien für die Speicherung zu verhindern.

Daher liegt der Anmeldung die Aufgabe zugrunde, ein Verfahren zum Betreiben eines Speichersystems zum effizienten Speichern von Datensätzen bereitzustellen, bei dem die Sicherheit verbessert und insbesondere der hierzu erforderliche Aufwand reduziert ist.

Die Aufgabe wird gemäß einem ersten Aspekt der Anmeldung durch ein Verfahren zum Betreiben eines dezentralen Speichersystems nach Anspruch 1 gelöst. Das dezentrale Speichersystem umfasst mindestens ein Peer-to-Peer Netzwerk mit mindestens einer Peer-to-Peer Anwendung. Das Verfahren umfasst:

- Empfangen, durch die Peer-to-Peer Anwendung, mindestens eines Datensatzes, der eine Speicherungsinformation umfasst, von einer Datenquelle,
- Ausführen eines Speicherungssteuermittels der Peer-to-Peer Anwendung durch mindestens einem Teil der Peer-Computer des Peer-to-Peer-Netzwerks, derart, dass basierend auf der Speicherungsinformation des Datensatzes und einem vorgegebenen Speicherungsvergleichskriteriums mindestens eine Speicheranordnung, in der der Datensatz gespeichert werden wird, aus zumindest zwei verfügbaren unterschiedlichen Speicheranordnungen durch das Speicherungssteuermittel bestimmt wird.

lndem im Gegensatz zum Stand der Technik anmeldungsgemäß ein Peer-to-Peer-Netzwerk, also eine dezentrale Struktur, mit einer Mehrzahl von Peer-Computern vorgesehen ist, auf denen eine Peer-to-Peer Anwendung (jeweils) installiert ist, wird die Sicherheit im Vergleich zu einer zentralen lnstanz signifikant verbessert. lnsbesondere wird eine verbesserte Sicherheit dadurch bereitgestellt, dass die Peer-to-Peer Anmeldung ein Speicherungssteuermittel umfasst, das durch mindestens einen Teil der Peer-Computer des Peer-to-Peer-Netzwerks derart ausgeführt wird, dass basierend auf der Speicherungsinformation des Datensatzes und einem (z.B. implizit oder vorzugsweise explizit) vorgegebenen Speicherungsvergleichskriteriums mindestens eine Speicheranordnung, in der der Datensatz gespeichert werden soll bzw. wird, aus zumindest zwei verfügbaren unterschiedlichen Speicheranordnungen durch das Speicherungssteuermittel bestimmt wird.

Mit anderen Worten ist anmeldungsgemäß anstelle eines zentralen Steuerungsservers oder einer entsprechenden Plattform ein Peer-to-Peer-Netzwerk (also ein Framework) vorgesehen, bei dem zumindest ein Teil (>1) der Peer-Computer des Peer-to-Peer-Netzwerks zumindest die Überwachung, vorzugsweise die Steuerung des Speicherungsvorgangs ausführt. Bei einem Peer-to-Peer-Netzwerk werden hohe Sicherheitsstandards dadurch erreicht, dass vorzugsweise sämtliche Peer-Computer bzw. Rechner (Peer-Knoten bzw. Peers) des Netzwerks, zumindest eine Teilmenge der Peer-Computer des Netzwerks, die Korrektheit des Bestimmungsvorgangs, insbesondere der aus dem Bestimmungsvorgang resultierenden Speicheranordnung, zumindest überwacht/en. Die Transaktionskosten können signifikant reduziert werden. Es ist keine zentrale, übergeordnete Plattform, Server, Cloud, etc. erforderlich. lnsbesondere ist in dem dezentralen Speicherungssystem keine zentrale lnstanz vorhanden.

Das Verfahren ist dazu konfiguriert, mindestens ein dezentrales Speichersystem zu betreiben. Das dezentrale Speichersystem umfasst mindestens ein Peer-to-Peer Netzwerk. Ein Peer-to-Peer Netzwerk umfasst eine Mehrzahl von Peer-Computern. Zwischen den Peer-Computern sind Kommunikationsverbindungen (z.B. lnternet) vorgesehen. Eine Mehrzahl von Peer-Computern, vorzugsweise jeder Peer-Computer des Peer-to-Peer Netzwerk, weist die (gleiche) Peer-to-Peer Anwendung, insbesondere eine Software-Anwendung, auf.

Das Verfahren umfasst das Empfangen von Datensätzen von mindestens einer Datenquelle. Vorzugsweise können eine Mehrzahl von Datenquellen, wie Sub-Datenquellen, vorgesehen sein, von denen ein oder mehrere Datensatz/sätze durch die Peer-to-Peer Anwendung empfangen werden können. Beispielhafte und nicht abschließende Datenquellen sind Komponenten eines Windparks (z.B. Offshore-Windparks), insbesondere Windkraftanlagen bzw. deren Sensoren, Messbojen, Energiekabel, Substationen etc., loT (lnternet of Things) Vorrichtungen, autonome Agenten, Chat Bots, Nutzerschnittstellen, (z.B. Tastatur (z.B. Software oder Hardware

eines mobilen Endgeräts), Biometrie Scanner, Spracherkennungsmodule, Videoanalysetools oder Gesichtserkennungsmodule), Speicheranordnungen etc. lnsbesondere kann die Datenquelle ein Sensor eines zuvor beschriebenen Geräts/Moduls/Komponente/etc. sein. Der Vorteil eines autonomen Agenten besteht darin, dass dieser Al (Künstliche lntelligenz) Software umfassen und autonom die Speicherungsinformation und/oder das Speicherungskriterium vorgeben kann.

Das Empfangen von mindestens einem Datensatz durch die Peer-to-Peer Anwendung umfasst insbesondere, dass der Datensatz von einem der Datenquelle zugeordnetem Peer-to-Peer Modul empfangen wird. Mit anderen Worten kann die Datenquelle Datensätze an die Peer-to-Peer Anwendung unter Nutzung eines Peer-to-Peer Moduls übertragen. Ein Peer-to-Peer-Modul ist insbesondere zum Kommunizieren mit der mindestens einen Peer-to-Peer Anwendung eingerichtet.

Ein Peer-to-Peer-Modul kann mindestens einer (eindeutig) Datenquelle zugeordnet sein. Beispielsweise kann die Datenquelle, insbesondere ein Gehäuse der Datenquelle, ein Peer-to-Peer-Modul umfassen. Vorzugsweise ist jedes Peer-to-Peer-Modul eindeutig einer jeweiligen Datenquelle zugeordnet. Beispielsweise kann das Peer-to-Peer-Modul in der Datenquelle, insbesondere in dem Gehäuse der Datenquelle, integriert sein.

Es ist auch möglich, dass eine Kommunikationsverbindung zwischen der Datenquelle und einem (entfernt von der Datenquelle angeordneten) Peer-to-Peer-Modul vorgesehen ist, welches dieser Datenquelle zugeordnet ist. Dies bedeutet insbesondere, dass das Peer-to-Peer-Modul zumindest im Namen der Datenquelle kommunizieren und/oder handeln kann. Beispielsweise kann das Peer-to-Peer-Modul teilweise durch eine separate Verarbeitungseinrichtung, wie beispielsweise ein mobiles Kommunikationsgerät (z. B. Mobiltelefon, mobiler Computer usw.), oder auf einer entfernten stationären Verarbeitungseinrichtung (z.B. ein Rechenzentrum) gebildet sein. lm Falle eines mobilen Kommunikationsgeräts oder einer entfernt angeordneten stationären Verarbeitungseinrichtung kann die mindestens eine

Datenquelle einen sicheren Kommunikationskanal zur Verarbeitungseinrichtung (oder Mobilkommunikationseinrichtung) des Rechenzentrums aufweisen und die Verarbeitungseinrichtung selbst kann eine Verbindung zum Peer-to-Peer-Netzwerk bereitstellen. ln einer Ausführungsform kann die entfernte Verarbeitungseinrichtung ein "Gateway" zum Peer-to-Peer-Netzwerk sein. Dies bedeutet, dass die Datenquelle über das zugeordnete Peer-to-Peer-Modul und das hierdurch gebildete Gateway sicher mit dem Peer-to-Peer-Netzwerk kommunizieren kann.

lm Vergleich zu einem Client-Server-Netzwerk, bei dem ein Server einen Dienst anbietet und ein Client diesen Dienst nutzt, ist in einem Peer-to-Peer-Netzwerk diese Rollenverteilung aufgehoben. Jeder Teilnehmer des Peer-to-Peer-Netzwerks kann einen Dienst gleichermaßen nutzen und selbst anbieten. lnsbesondere ist ein Peer-to-Peer-Netzwerk selbstbestimmt und/oder selbstorganisiert (ohne übergeordnete Einheit). Vorliegend weist vorzugweise jeder Peer-Computer bzw. Peer des Peer-to-Peer-Netzwerks eine Peer-to-Peer- Anwendung auf.

Die Peer-to-Peer Anwendung weist zumindest ein Speicherungssteuermittel auf. Das Speicherungssteuermittel kann insbesondere ein ausführbares Softwaremodul sein. lnsbesondere kann die Ausführung des mindestens einen Speicherungssteuermittels (automatisch) initiiert werden, wenn die Peer-to-Peer Anwendung einen Datensatz empfängt.

Nach dem Empfang des Datensatzes wird der Speicherort für diesen Datensatz in einem Bestimmungsvorgang bestimmt. lnsbesondere wird die Speicheranordnung aus einer Mehrzahl von verfügbaren Speicheranordnungen bestimmt, in der der Datensatz gespeichert werden soll bzw. in der die Speicherung des Datensatzes gewünscht ist.

Die Bestimmung umfasst insbesondere das Auswerten einer Speicherungsinformation des empfangenen Datensatzes und eines vorgegebenen Speicherungsvergleichskriteriums, das beispielsweise in der Peer-to-Peer Anwendung gespeichert sein kann. lndem der Datensatz mit einer Speicherungsinformation

versehen ist, aus der ein gewünschter Speicherort und/oder ein gewünschtes Speichersicherheitslevel (zusammen mit dem Speicherungsvergleichskriterium) abgeleitet werden kann, kann das Speicherungssteuermittel die Speicheranordnung bestimmen, in der der Datensatz gespeichert werden soll.

Vorzugsweise können die mindestens zwei verfügbaren, unterschiedlichen Speicheranordnung eine erste und mindestens eine weiteren Speicheranordnung umfassen, wobei die erste Speicheranordnung im Relation zu der mindestens einen weiteren verfügbaren Speicheranordnung eine erhöhte Speichersicherheit bzw. ein höheres Speichersicherheitslevel für die Datensätze bereitstellt. Die erste Speicheranordnung kann insbesondere als sicheres Langzeitgedächtnis implementiert sein, welches z.B. ein revisionssicheres Speichern von Datensätzen erlaubt. Die mindestens eine weitere Speicheranordnung kann als ein unsichereres Kurzzeitgedächtnis konfiguriert sein. Das Vorgeben von mindestens einem Speicherungsvergleichskriteriums kann das Zuordnen des Datensatzes für eine Speicherung zu dem ersten oder der mindestens einen weiteren Speicheranordnung ermöglichen.

Wie bereits beschrieben wurde, kann das mindestens eine Speicherungssteuermittel durch zumindest einem Teil der Peer-Computer ausgeführt werden. Nur wenn dieser Teil zu dem gleichen Bestimmungsergebnis (also z.B. jeweils die gleiche Speicheranordnung bestimmt wird) gelangt, wird eine Speicheranordnung (tatsächlich) für die Speicherung des entsprechenden Datensatzes bestimmt. Hierdurch kann die Manipulationssicherheit erhöht werden, da die Manipulation von beispielsweise einem Peer-Computer des Teils der Peer-Computer detektiert wird. lnsbesondere wird dann das Bestimmungsergebnis durch den Teil der Peer-Computer nicht eindeutig sein.

Unter dem Ausführen eines Mittels (z.B. Speicherungssteuermittels) durch einen Teil der Peer-Computer ist vorliegend zu verstehen, dass zumindest zwei oder mehr Peer-Computer jeweils das Mittel (z.B. Speicherungssteuermittel) ausführen und nur bei

einem gleichem Ausführungsergebnis durch diese Peer-Computer eine bestimmte Handlung (z.B. Bestimmen der Speicheranordnung) bewirkt wird oder mindestens ein Peer-Computer das Mittel (z.B. Speicherungssteuermittel) (komplett) ausführt und mindestens ein weiterer Peer-Computer eine dem Mittel (z.B. Speicherungssteuermittel) zugeordnetes Überprüfungsmittel ausführt, um die Korrektheit der Ausführung des Mittels (z.B. Speicherungssteuermittel) zu bestätigen bzw. zu überwachen.

Nach einer Bestimmung der Speicheranordnung kann insbesondere vorgesehen sein, dass eine Weiterleitung des empfangenen Datensatzes für eine Speicherung des Datensatzes an die bestimmte Speicheranordnung durch das Speicherungssteuermittel bewirkt werden kann. Der weitergeleitete Datensatz wird dann von der Speicheranordnung gespeichert. Beispielhafte und nicht abschließende Speicheranordnungen sind Clouds, zentrale Datenbanken, dezentrale Datenbanken (Big lnterplanetary File System (1PFS) oder storj oder in einer verteilten Blockchain-Datenbank (z.B. BigChainDB oder mit Cryptowerk-Funktionen gehashte Datenbank, wie Anker-Hashing)). Hierbei weisen die (genannten) dezentralen Datenbanken einen höheren Speichersicherheitslevel im Vergleich zu den genannten Cloud-Datenbanken oder zentralen Datenbanken auf und können daher insbesondere als sicheres Langzeitgedächtnis genutzt werden. Das höhere Speichersicherheitslevel ergibt sich insbesondere dadurch, dass entweder die Daten in eine Blockchain-Datenbank unveränderbar („immutable") gespeichert werden oder die Daten gehasht werden und der Hash oder ein Anker-Hash von einem Paket von Data-Sets auf einer (oder mehreren) Blockchain oder Blockchain-Datenbank (en) gespeichert werden, so dass zu einem späteren Zeitpunkt die lntegrität der Daten (eindeutig) überprüft werden kann.

Ferner kann vorzugsweise eine Mehrzahl von Speicherungssteuermitteln in einer und/oder mehreren Peer-to-Peer Anwendung/en vorgesehen sein, die zumindest teilweise parallel von dem (jeweiligen) Peer-Computern ausgeführt werden können. Dies ermöglicht eine parallele Verarbeitung von einer Mehrzahl an Datensätzen durch die Peer-to-Peer Anwendung.

Zudem kann vorgesehen sein, dass einzelne (dezentrale) Speicheranordnungen nach Prinzipien der Public, Private, Consortium oder permissionless oder permissioned oder einer Hybrid-Form organisiert sind. Für zentrale Speichermedien kann vorgesehen sein, dass verschiedene Varianten genutzt werden (z.B. Private On-Premise Data Storage, Public Data Storage, Cloud Data Storage, etc.).

Gemäß einer ersten Ausführungsform des anmeldungsgemäßen Verfahrens kann die empfangene Speicherungsinformation ein Speicherungskriterium sein und/oder es kann aus der empfangenen Speicherungsinformation ein Speicherungskriterium bestimmbar bzw. ableitbar sein. Das Bestimmen der Speicheranordnung kann auf einem Vergleich des Speicherungskriteriums und des Speicherungsvergleichskriteriums basieren. lndem die Speicherungsinformation ein (unmittelbares) Speicherungskriterium (z.B. eine bestimmte bit-Folge und/oder eine gesetzte bzw. nicht gesetzte Flag) aufweist, kann der Speicherungsort bzw. die gewünschte Speicheranordnung direkt aus dem Speicherungskriterium bestimmt werden. Beispielsweise kann die Speicheranordnung in der Speicherungsinformation direkt angegeben sein (z.B. eine Speicheranordnungskennung) oder ein gewünschtes Speichersicherheitslevel. lnsbesondere durch einen (zumindest impliziten) Vergleich mit dem vorgegebenen Speicherungsvergleichskriteriums (z.B. Speicheranordnungskennungen der verfügbaren Speicheranordnungen und/oder eine Flaginformation) kann die Speicheranordnung, in der der Datensatz gespeichert werden wird, von dem Speicherungssteuermittel bestimmt werden. Auch kann vorgesehen sein, dass aus der Speicherungsinformation (z.B. eine Adresse und/oder Kennung) das Speicherungskriterium abgeleitet werden kann. Beispielsweise kann auf die angegebene Adresse (oder Kennung) durch das Speicherungssteuermittel zugegriffen werden, um das an der Adresse hinterlegte Speicherungskriterium auszulesen. ln einfacher Weise kann die gewünschte Speicheranordnung bestimmt werden.

Gemäß einer weiteren Ausführungsform kann mindestens ein zumindest von der Peer-to-Peer-Anwendung kontrollierbares Hashmittel vorgesehen sein. Das Verfahren kann ferner umfassen:

- Ausführen des Hashmittels, insbesondere durch mindestens einen Teil der Peer-Computer des Peer-to-Peer-Netzwerks, derart, dass der empfangene Datensatz (vor einer Speicherung in der bestimmten Speicheranordnung) gehasht wird (und / oder dass ein von einer Datenquelle mitgelieferter Hashwert überprüft wird), und insbesondere
- Bewirken einer Weiterleitung des gehashten Datensatzes an die bestimmte Speicheranordnung für eine Speicherung des gehashten Datensatzes durch das Speicherungssteuermittel.

lndem der mindestens eine Datensatz zunächst gehasht wird, wird eine Durchsuchbarkeit der gespeicherten Datensätze in einer Speicheranordnung ermöglicht. Zudem kann eine kryptographische Speicherung der Datensätze erfolgen, so dass insbesondere zu einem späteren Zeitpunkt unter Verwendung eines Hashes oder eines Anker-Hash Verfahrens mit Anker-Hash und Smart Stamp (Smart Stamp wird bei einigen Verfahren benötigt, um bei Nutzung eines Data Sets aus einem Datenpacket unter Zuhilfenahme von Anker-Hash und Smart Stamp mit einem Verifikationsalgorithmus zu überprüfen) die lntegrität der Daten überprüft werden kann. Das Speicherungssteuermittel kann steuern, an welchen Speicherorten Hashes, Anker-Hashes und/oder Smart Stamps gespeichert werden, und es kann insbesondere einzelne Datensätze mit den Adressen, Hashes, Anker-Hashes und Smart Stamps verknüpfen und/oder hierfür ein Register erstellen.

Vorteilhafterweise sind vorzugsweise sämtliche Datenquellen, die Datensätze an das dezentrale Speichersystem übertragen können, in einem Register registriert. Das Register kann in der Peer-to-Peer Anwendung und/oder in einer Speicheranordnung implementiert sein. lnsbesondere können neue Datenquellen durch einen von der Peer-to-Peer Anwendung zumindest kontrollierbaren Registriervorgang (z.B. durch ein Registriermittel) in dem mindestens einen Register registriert werden. Gemäß

einer bevorzugten Ausführungsform kann die mindestens eine Datenquelle in einem von der Peer-to-Peer Anwendung zumindest kontrollierbaren Register registriert sein oder werden. Das Registrieren der Datenquelle in dem Register kann zumindest das Speichern einer Datenquellenkennung der Datenquelle als Speicherungsinformation und das Speichern eines der Datenquellenkennung zugeordneten Speicherungskriterium in dem Register umfassen.

Eine Datenquellenkennung ist insbesondere einer Datenquelle direkt oder indirekt (z.B. über das zugeordnete Peer-to-Peer Modul) eindeutig zugeordnet. Mit anderen Worten kann die Datenquelle in dem vorliegenden System eindeutig durch die Datenquellenkennung identifiziert werden. ln dem Register kann einer Datenquellenkennung mindestens ein Speicherungskriterium für die von dieser Datenquelle empfangenen Datensätze zugeordnet werden. Das Speicherungskriterium ist insbesondere eine Angabe über den (gewünschten) Speicherort oder die (gewünschte) Speicheranordnung oder den (gewünschten) (Mindest-)Speichersicherheitslevel, in der der jeweilige Datensatz gespeichert werden wird.

Das Speicherungssteuermittel kann zunächst als Speicherungsinformation die Datenquellenkennung eines empfangenen Datensatzes auslesen. Durch einen Zugriff auf das Register unter Nutzung der Datenquellenkennung und insbesondere durch Durchführen einer Vergleichsoperation zwischen der ausgelesenen Datenquellenkennung und den registrierten Datenquellenkennungen kann das zugehörige Speicherungskriterium abgeleitet bzw. bestimmt werden. Beispielsweise kann das Speicherungskriterium eine Speicheranordnungskennung und/oder eine Angabe für ein gewünschtes Speichersicherheitslevel sein. Durch einen (impliziten) Vergleich mit vorgegebenen Speicheranordnungskennungen und/oder von den mindestens zwei Speicheranordnungen zur Verfügung gestellten (unterschiedlichen) Speichersicherheitsleveln kann die Speicheranordnung bestimmt werden.

Es versteht sich, dass von einer Datenquelle unterschiedliche Datensatzarten empfangen werden können, die in unterschiedlichen Speicheranordnungen gespeichert werden können. Hierfür kann der Datenquellenkennung mindestens eine Datensatzartkennung (z.B. zwei oder mehr) zugeordnet sein. Der mindestens einen Datensatzartkennung kann wiederum (jeweils) mindestens ein Speicherungskriterium zugeordnet sein. ln diesem Fall kann die Speicheranordnung basierend auf der Datenquellenkennung und der Datensatzartkennung bzw. das aus diesen Kennungen (eindeutig) ableitbare Speicherungskriterium bestimmt werden (wie zuvor beschrieben wurde).

Wie bereits beschrieben wurde, kann gemäß einer Ausführungsform das Bestimmen der Speicheranordnung ein Bestimmen eines gespeicherten Speicherungskriterium basierend auf einem Vergleich der Speicherungsinformation (Datenquellenkennung und/oder Datensatzartkennung) des empfangenen Datensatzes mit den in dem Register gespeicherten Speicherungsinformationen (Datenquellenkennung und/oder Datensatzartkennung) umfassen. Das Bestimmen der Speicheranordnung kann auf dem bestimmten Speicherungskriterium basieren.

Die Speicherungsinformation kann weitere Daten, wie Datentyp, Senderangaben etc. umfassen, die bei dem Bestimmungsvorgang berücksichtigt werden können.

Darüber hinaus kann das Hashmittel vorzugsweise ein Anker-Hashmittel sein. Die von dem Anker-Hashmittel für einen von einer bestimmten Datenquelle empfangenen Datensatz erzeugten Anker-Hashwerte können, basierend auf einer in dem Register gespeicherten Anker-Hashspeicherungsinformation, die der Datenquellenkennung der bestimmten Datenquelle zugeordnet sein kann, gespeichert werden. lnsbesondere umfasst dies die Speicherung der Ankerhashwerte in einer Speicheranordnung und/oder einer Peer-to-Peer Anwendung entsprechend der Ankerhashspeicherungsinformation.

Vorzugsweise kann ein empfangener Datensatz, insbesondere dessen Roh-Daten, mit Metadaten kombiniert und der resultierende Datensatz durch das Anker-Hashmittel gehasht werden. Bei den Metadaten kann es sich insbesondere um Metadaten des für den Empfang aufgebauten Kommunikationskanal (z.B. der verwendete Kommunikationskanal, eingesetztes Authentifizierungs- und/oder Kommunikations-Protokoll (z.B. TLS, SSL, IOTA MAM), lnformationen zur Qualität der Kommunikationsverbindung, Zeitstempel etc.) handeln. Auch können die Metadaten auch Angaben über die Art der Daten (z.B. Temperatur mit einer Auflösung von X und gemessen in °C (oder K)) umfassen. Vorzugsweise kann eine Object Memory Modellig (OMM) Methode angewendet werden, um die Metadaten in einem standardisierten Format zu speichern, welches insbesondere anderen Entitäten die Weiterverarbeitung ermöglicht. ln einer bevorzugten Ausführungsform kann die OMM Methode kombiniert mit einem Text2Binary Modul, welches die OMM Datensätze für eine effiziente Speicherung in kürzeren Binär-Code transformiert und / oder komprimiert, eingesetzt werden.

Die Ankerhashwerte (welche die Adressdaten der gespeicherten Daten des Datensatzes und/oder Adresse des Smart Stamps umfassen) werden insbesondere entsprechend der Ankerhashspeicherungsinformation, die einer Datenquellenkennung und/oder einer Datensatzartkennung in dem Register zugeordnet ist, gespeichert. lnsbesondere kann das Anker-Hashmittel (z.B. entsprechend den vorherigen Ausführungen zu dem Speicherungssteuermittel) bei einem Empfang eines Datensatzes auf das Register mittels der zuvor genannten Kennungen zugreifen und beispielsweise die entsprechende Ankerhashspeicherungsinformation bestimmen bzw. ableiten. Die Ankerhashspeicherungsinformation gibt hierbei insbesondere die Speicheranordnung und/oder Peer-to-Peer Anwendung an, in der mindestens eine Ankerhashwert gespeichert werden wird bzw. soll.

Das Hashmittel, insbesondere das Anker-Hashmittel, kann ein Hashmittel der Peer-to-Peer Anwendung sein und insbesondere von zumindest einem Teil der Peer-

Computer (entsprechend den vorherigen Ausführungen zu dem Speicherungssteuermittel) ausgeführt werden. Alternativ oder zusätzlich kann das Hashmittel, insbesondere das Anker-Hashmittel, auf einer Offchain-Rechenvorrichtung (z.B. dezentraler „computation market") oder einen Trusted Computing Gerät (z.B. SGX oder Software Secure Enclave), die/das von der Peer-to-Peer Anwendung gesteuert wird, ausgeführt werden.

Gemäß einer weiteren bevorzugten Ausführungsform des anmeldungsgemäßen Verfahrens kann das Verfahren ferner umfassen:

- Bestimmen eines Datensatzwerts und/oder eines Datenquellenwerts in einem Bewertungsschritt,
- Vergleichen des bestimmten Datensatzwerts und/oder Datenquellenwerts mit mindestens einem (entsprechenden) vorgegebenen Vergleichswert, und
- Bewirken einer Änderung des Speicherungskriteriums und/oder des Speicherungsvergleichskriteriums für einen entsprechenden Datensatz abhängig von dem Vergleichsergebnis.

Das Bestimmen des mindestens einen Speicherwerts bzw. Datensatzwerts und/oder des Datenquellenwerts von mindestens einem Datensatz und/oder mindestens einer Datenquelle kann insbesondere ein Bestimmen von mindestens einem gespeicherten Datensatz oder von mehreren Datensätzen einer bestimmten Datensatzart und/oder von mehreren Datensätzen mindestens einer bestimmten Datenquelle (z.B. mehrerer Datenquellen gleicher Datenquellenart) umfassen.

Anmeldungsgemäß ist erkannt worden, dass sich während des Betriebs des dezentralen Speichersystems die Sicherheitsanforderung für das Speichern von einem Datensatz ändern kann. Anmeldungsgemäß wird daher gemäß dieser Ausführungsform vorgeschlagen, eine (automatische) Regelung zu implementieren, um bei Detektion einer geänderten Sicherheitsanforderung für Datensätze einer bestimmten Datenquelle und/oder einer bestimmten Datensatzart eine Anpassung des Bestimmungsvorgangs zu bewirken.

lnsbesondere kann eine Änderung der Sicherheitsanforderung durch ein Bestimmen eines Datensatzwerts und/oder eines Datenquellenwerts von mindestens einem gespeicherten Datensatz mindestens einer bestimmten Datenquelle oder von einer bestimmten Datensatzart (von beispielsweis mehrere Datenquellen) detektiert werden. Hierbei ist der Datensatzwert und/oder der Datenquellenwert insbesondere ein lndiz für die augenblickliche Sicherheitsanforderung des Datensatzes, der Datensatzart und/oder der Datenquelle.

Ferner kann mindestens ein Vergleichswert (z.B. Datensatzvergleichswerts und/oder Datenquellenvergleichswert) vorgeben sein, der eine augenblickliche Einstufung der Sicherheitsanforderung ermöglicht. Beispielsweise kann ein Grenzwert vorgegeben sein. Übersteigt der bestimmte Datensatzwerts und/oder der Datenquellenwert den Grenzwert, kann beispielsweise ein erhöhter Speichersicherheitslevel bestimmt werden. Wird der Grenzwert unterschritten, kann beispielsweise ein niedrigerer Speichersicherheitslevel bestimmt werden. Es versteht sich, dass mehr als zwei Speichersicherheitslevels mit einer entsprechenden Mehrzahl von Grenz- bzw. Vergleichswerten vorgesehen sein können.

Wird hierbei festgestellt, dass sich der Datensatzwert und/oder der Datenquellenwert insbesondere im Laufe der Zeit derart verändert hat, dass der Vergleichswert (im Vergleich zur Vergangenheit nun) überschritten bzw. unterschritten wird, kann eine Änderung des Speicherungskriteriums und/oder des Speicherungsvergleichskriteriums abhängig von dem Vergleichsergebnis bewirkt werden. Beispielsweise kann das in dem Register für diesen Datensatz, diese Datensatzquelle und/oder diese Datensatzart gespeicherte Speicherungskriterium angepasst werden. Alternativ oder zusätzlich kann das vorgegeben Speicherungsvergleichskriterium angepasst werden. Auch ist es möglich, dass die entsprechende Datenquelle veranlasst wird, die Speicherungsinformation (z.B. das Speicherungskriterium), mit der der Datensatz versehen wird, zu ändern.

Der Bewertungsschritt kann mehrmals, beispielsweise regelmäßig, durchgeführt werden. lndem insbesondere regelmäßig überprüft wird, welche Sicherheitsanforderung an Datensätze augenblicklich gestellt werden, kann der verfügbare Speicherplatz in den Speicheranordnungen effizient genutzt werden. So können anmeldungsgemäß nur Datensätze in einer ersten Speicheranordnung gespeichert werden, die einen hohen Speichersicherheitslevel (im Vergleich zu mindestens einer weiteren Speicheranordnung) bereitstellt, wenn dieser Level auch tatsächlich erforderlich ist. Kosten können reduziert werden.

Der Bewertungsvorgang kann vorzugsweise durch mindestens ein Bewertungsmittel der Peer-to-Peer Anwendung durchgeführt werden. Das Bewertungsmittel kann zumindest von einem Teil der Peer-Computer (entsprechend den vorherigen Ausführungen zu dem Speicherungssteuermittel) ausgeführt werden. Alternativ oder zusätzlich kann das Bewertungsmittel auf einer Offchain-Rechenvorrichtung oder einen Trusted Computing Gerät (z.B. SGX oder Software Secure Enclave), die/das von der Peer-to-Peer Anwendung gesteuert wird, ausgeführt werden.

Vorzugsweise zusätzlich hierzu kann gemäß einer weiteren Ausführungsform des anmeldungsgemäßen Verfahrens der mindestens eine bewertete Datensatz (z.B. alle Datensätze einer Datensatzart und/oder einer bestimmten Datenquelle) abhängig von dem Vergleichsergebnis von einer ersten Speicheranordnung in eine weitere Speicheranordnung (oder umgekehrt) verschoben werden. Die erste Speicheranordnung kann in Relation zu der weiteren Speicheranordnung eine andere Speichersicherheit bzw. eine anderes Speichersicherheitslevel bereitstellen. Hierdurch kann der verfügbare Speicherplatz besonders effizient genutzt werden.

Grundsätzlich kann ein Datensatzwert eines Datensatzes oder einer Datensatzart oder ein Datenquellenwert einer (bestimmten) Datenquelle auf verschiedene Weise bestimmt werden. Gemäß einer Ausführungsform kann das Bestimmen des Datensatzwerts und/oder des Datenquellenwerts von mindestens einem gespeicherten Datensatz (oder von mehreren Datensätzen der bestimmten

Datenquelle) das Auswerten von Zugriffszahlen auf den mindestens einen Datensatz (insbesondere während eines bestimmten Zeitintervalls) umfassen. Anschließend kann die bestimmte Zugriffszahl mit einem entsprechenden, vorgegebenen Vergleichswert entsprechend den obigen Ausführungen verglichen werden. Dann kann ggf. eine zuvor beschriebene Änderung des Speicherungskriteriums und/oder des Speicherungsvergleichskriteriums erfolgen.

Die Zugriffszahl kann insbesondere die Anzahl an Zugriffen auf einen Datensatz, eine Datensatzart oder Datensätze einer bestimmten Datenquelle, beispielsweise innerhalb einer vorgegebenen Zeitdauer, repräsentieren.

Alternativ oder zusätzlich kann das Bestimmen des Datensatzwerts und/oder Datenquellenwerts von einem gespeicherten Datensatz oder von mehreren Datensätzen der bestimmten Datenquelle das Auswerten eines Zugriffskriteriums umfassen, das für einen Zugriff auf den Datensatz oder auf die mehreren Datensätze der bestimmten Datenquelle erfüllt werden muss. Anschließend kann das bestimmte Zugriffskriteriums mit einem entsprechenden, vorgegebenen Vergleichswert entsprechend den obigen Ausführungen verglichen werden. Dann kann ggf. eine zuvor beschriebene Änderung des Speicherungskriteriums und/oder des Speicherungsvergleichskriteriums erfolgen.

Alternativ oder zusätzlich kann das Bestimmen des Datensatzwerts und/oder Datenquellenwerts von einem gespeicherten Datensatz oder von mehreren Datensätzen der bestimmten Datenquelle das Auswerten von Sicherheitsparametern und/oder Schutzparametern des Datensatzes und/oder der bestimmten Datenquelle umfassen (z.B. Wert von Daten auf einem Data Market Exchanges im Vergleich zum Risiko des Datenverlustes oder des Auftretens von Datenmanipulation auf einem Datenspeichertyp, Wert für Safety und Security von Personen, Objekten oder Maschinen).

Darüber hinaus können gemäß einer weiteren Ausführungsform die gespeicherten Datensätze der mindestens einen Datenquelle/n in Abhängigkeit eines (vorgebbaren) Analysealgorithmus in einem Auswerteschritt ausgewertet werden. Mindestens ein neuer Datensatz kann basierend auf dem Auswerteergebnis generiert und in einer Speicheranordnung gespeichert werden. Der Analysealgorithmus kann insbesondere vorgegeben sein. Ein Auswertemittel, beispielsweise der Peer-to-Peer Anwendung, kann basierend auf dem vorgegebenen Analysealgorithmus eine Auswertung durchführen. Das Auswertemittel kann von zumindest einem Teil der Peer-Computer (entsprechend den vorherigen Ausführungen zu dem Speicherungssteuermittel) ausgeführt werden. Alternativ oder zusätzlich kann das Auswertemittel auf einer Offchain-Rechenvorrichtung oder einen Trusted Computing Gerät (z.B. SGX oder Software Secure Enclave), die/das von der Peer-to-Peer Anwendung gesteuert wird, ausgeführt werden.

Vorzugsweise kann dem in dem Auswerteschritt verwendeten Analysealgorithmus eine (eindeutige) Algorithmuskennung zugeordnet werden. Der Analysealgorithmus kann zusammen mit der Algorithmuskennung gespeichert werden (z.B. in einer Speicheranordnung). Der erzeugte Datensatz kann zusammen mit der Algorithmuskennung des Analysealgorithmus, der für die Erzeugung des Datensatzes verwendet wurde, gespeichert werden. Hierdurch kann erreicht werden, dass die Generierung des neuen Datensatzes für Dritte nachvollziehbar ist.

Vorzugsweise können Datensätze von zwei oder mehr eine Gruppe bildenden Datenquellen (z.B. Datenquellen gleicher Datenquellenart (z.B. Windkraftanlagen eines Windparks, Fahrzeuge einer Fahrzeugflotte etc.)) ausgewertet werden. Das Auswerteergebnis kann der Gruppe der Datenquellen zugeordnet und insbesondere zusammen mit der Gruppenkennung der Gruppe gespeichert werden. Beispielsweise kann die Gruppe (z.B. Flotte, System, Produkt bestehend aus Komponenten, Palette mit Produkten) und die zugehörige Gruppenkennung, z.B. durch das Auswertemittel, neu generiert werden. Dann können die Datensätze der einzelnen Datenquellen dieser Gruppe entsprechend vorgebbarer Analysealgorithmen ausgewertet und die

Auswerteergebnis als neue Datensätze gespeichert werden, wobei sie der Gruppenkennung zugeordnet werden können.

Gemäß einer weiteren Ausführungsform kann ein Datensatz bei einer Verbindungsunterbrechung zwischen der Datenquelle und der Peer-to-Peer-Anwendung in einem lokalen Speicher der Datenquelle gespeichert werden. Der in dem lokalen Speicher gespeicherte Datensatz kann bei Detektion einer Aufhebung der Verbindungsunterbrechung an die Peer-to-Peer Anwendung übertragen werden. Hierdurch kann erreicht werden, dass auch bei einer Verbindungsunterbrechung zwischen Peer-to-Peer Netzwerk und Datenquelle keine Daten verloren gehen. Die Datensicherheit wird weiter verbessert.

Darüber hinaus kann das Register zumindest ein Teil einer Speicheranordnung darstellen. lnsbesondere können die von einer Datenquelle (z.B. Windkraftanlage, Komponenten einer Windkraftanlage, Fahrzeug, Komponente eines Fahrzeugs etc.) stammenden Datensätzen der Datenquellenkennung zugeordnet sein. lnsbesondere kann von der Datenquelle ein so genannter „digitaler Zwilling" („digital twin") erstellt werden.

Vorzugsweise können bereits während des Registrierungsvorgangs einer Datenquelle Datenquellenparameter (z.B. Speicherungskriterium, Ankerhashspeicherungsinformation, Hersteller der Datenquelle, Leistungs- und/oder Verbrauchsangaben der Datenquelle, Datenquellenart, Gruppenkennung der zugeordneten Gruppe, Reputation bzw. Qualität technischer Parameter, unterstützte Kommunikations- und/oder Dialogprotokolle für die Anbindung von Steuervorrichtungen und/oder Synchronisationsmodulen und/oder unterstützte Steuerungs- und/oder Synchronisationsmechanismen etc.) zusammen mit der Datenquellenkennung (und/oder Datensatzartkennung) abgespeichert werden.

Vorzugsweise kann die Peer-to-Peer Anwendung ein Konfigurationsmittel umfassen. Das Konfigurationsmittel kann von zumindest einem Teil der Peer-Computer

(entsprechend den vorherigen Ausführungen zu dem Speicherungssteuermittel) ausgeführt werden. Alternativ oder zusätzlich kann das Konfigurationsmittel auf einer Offchain-Rechenvorrichtung oder einen Trusted Computing Gerät (z.B. SGX oder Software Secure Enclave), die/das von der Peer-to-Peer Anwendung gesteuert wird, ausgeführt werden.

Das Verfahren kann gemäß einer weiteren Ausführungsform umfassen:

- Bewirken einer Übertragung eines Konfigurationsdatensatzes an eine Datenquelle, insbesondere durch Ausführen des Konfigurationsmittels der Peer-to-Peer Anwendung durch mindestens einem Teil der Peer-Computer des Peer-to-Peer-Netzwerks.

Mit anderen Worten kann die Peer-to-Peer Anwendung nicht nur eine Filterfunktion für empfangene Datensätze von Datenquellen sein, sondern vorzugsweise zusätzlich eine Verteilerfunktion für Datensätze (insbesondere Konfigurationsdatensätze) sein, die an mindestens eine Datenquelle übertragen werden sollen. ln einfacher Weise können Konfigurationsdatensätze, wie Software-Updates, Steuerparameter etc., an die mindestens eine Datenquelle verteilt werden. Vorzugsweise können kryptographische Verfahren, wie z.B. Code Signing, Attestation, Sealing etc., für die Verteilung der Konfigurationsdatensätze verwendet werden. Vorzugweise können Authentizität, Provenance und/oder Reputation eines Konfigurationsdatensatzes in einem Register nachvollziehbar gespeichert werden, so dass insbesondere eine Datenquelle dies vor Annahme des Codes überprüfen kann.

Besonders bevorzugt kann ein Konfigurationsdatensatz bei einer Verbindungsunterbrechung zwischen der Datenquelle und der Peer-to-Peer Anwendung in der Peer-to-Peer Anwendung und/oder dem Register (unter Zuordnung zu der Datenquellenkennung der Datenquelle, an die der Datensatz übertragen werden soll/wird) gespeichert werden. Bei Detektion einer Aufhebung der Verbindungsunterbrechung kann die Übertragung des gespeicherten Konfigurationsdatensatzes an die Datenquelle durch Ausführen des

Konfigurationsmittels der Peer-to-Peer Anwendung, insbesondere durch mindestens einen Teil der Peer-Computer des Peer-to-Peer-Netzwerks, bewirkt werden.

Gemäß einer weiteren Ausführungsform kann ein empfangener Datensatz verschlüsselt in einer Speicheranordnung gespeichert werden. Zur Verschlüsselung kann insbesondere das Proxy-re-Encryption-Verfahren verwendet werden. Alternativ oder zusätzlich kann für die Schlüsselverwaltung einer Verschlüsselung des mindestens einen Datensatzes insbesondere das Multi-Party Computation (MPC) Verfahren verwendet werden.

Die Verwendung von Proxy-re-Encryption-Verfahren bringt insbesondere Vorteile für das Teilen der Datensätze, insbesondere von sensitiven Datensätzen sowie der Zugriffsverwaltung hierdrauf und die Umsetzung von GDPR (General Data Protection Regulation) (Regulation (EU) 2016/679) (z.B. Daten werden nicht gelöscht, sondern die Daten werden für die Proxy-re-encryption deaktiviert (z.B. durch eine Schreibtransaktion in einen Smart Contract einer Peer-to-Peeranwendung)). Die Deaktivierung kann dann als eine Transaktion gespeichert werden.

Zusätzlich kann Multi-Party Computation (MPC) für das Key Management genutzt werden. Dies hat den Vorteil, dass der Schlüssel nicht mehr auf einem Server oder einer anderen zentralen lnstanz gespeichert wird, sondern per MPC auf verschiedenen Peer-Computern des Peer-to-Peer Netzwerk, wobei jeweils nur Teile eines Schlüssels auf einem Peer-Computer gespeichert werden. Die Manipulationssicherheit kann noch weiter verbessert werden. Authentifizierung kann insbesondere parallel auf mehreren MPC Peer-Computern durchgeführt werden. Ein Peer-Computer weiß hierbei insbesondere nicht, welcher Art von Aufgabe er gerade ausführt.

Vorzugweise können ‚Authenticated Encryption' Verfahren in der Kommunikation zwischen einer Datenquelle und einer Speicheranordnung angewendet werden, um die Authentizität und Sicherheit der von der Datenquelle an die Speicheranordnung

kommunizierten Daten zu gewährleisten. Das Authenticated Encryption Verfahren kann mit einem ldentitätsregister gespeichert auf der Speicheranordnung sowie MPC und Proxy-Re-Encryption kombiniert werden.

ln einer bevorzugten Ausführungsform können, nach Parametern gesteuert, Snap-Shots oder Clones einer gesamten Speicheranordnung oder mindestens eines Teils der Speicheranordnung insbesondere in einer (zentralen) High-Performance Datenbank abgelegt (und die lntegrität der Daten mittels Hash-Werten überprüfbar gemacht) werden. Das kann den Vorteil haben, dass Algorithmen schnelleren Zugriff auf die Daten haben und größere Mengen pro Zeiteinheit analytisch verarbeiten können. ln vorzugsweise regelmäßigen Abständen oder pro Event kann ein solcher Snap-Shot oder Clone aktualisiert werden. Das Speicherungssteuermittel kann so konfiguriert werden, dass es die Snap-Shot oder Clone-Erstellung triggert. Dazu kann ein Snap-Shot oder Clone mit den Parametern in der Speicheranordnung registriert werden.

ln einer anderen Ausführung kann das Speicherungssteuermittel so konfiguriert sein, dass es per Pull-Mechanismen Daten von den Datenquellen aktiv abfragt. Dazu kann eine Datenquelle in einem Register mit den Parametern für Pull-Abfragen registriert sein (z.B. Häufigkeit, welche Daten, welche Kommunikationsprotokolle, Format der Daten, Batch-Abfragen, Flottenabfragen, etc.). Bevorzugt können auch Push-Mechanismen mit vergleichbaren Parametern registriert sein. Mit diesen lnformationen kann das Speicherungssteuermittel eine Voraussage über die benötigten Ressourcen für Computation, Key Management und Speichervolumina machen und diese reservieren bzw. benötigte lnfrastruktur konfigurieren sowie Load Balancing lnfrastruktur einbinden.

ln einer weiteren, besonders bevorzugten Ausführung kann in das Speicherungssteuermittel ein Quantum Random Number Generator (QRNG) bzw. ein Non-Algorithmic RNG integriert sein. Damit können für kryptographischen Verfahren benötigte Zufallszahlen erzeugt werden, die frei von möglichen algorithmischen Mustern sind. Damit wird die Anfälligkeit der kryptographischen Verfahren gegen

Angriffe noch weiter reduziert. Das Speicherungssteuermittel kann so konfiguriert sein, dass es von ihm erzeugte Zufallszahlen sicher an mindestens eine Datenquelle verteilt, so dass insbesondere die mindestens eine Datenquelle die erzeugten Zufallszahlen für die Sicherung kryptographischer Verfahren benutzen können.

ln einer weiteren Ausführung gibt es ein Register („Registry") für die Speicheranordnungen bzw. Datenspeicher, d.h. Datenspeicher des Systems können in einem primären Datenspeicher registriert (Geographische Lokation des Datenspeichers, Validierung der Lokation, Volumina, Kosten, Latenzzeiten, Datenbanktyp, Sharding, SLAs, zeitliche Verfallsdaten, etc.) werden.

ln einer weiteren Ausführungsform kann ein Datenspeicher sogenannte Sharding Verfahren verwenden. Das Speicherungssteuermittel kann so konfiguriert sein, dass es Daten - gemäß einer in einem Register für Datenspeicher und/oder Datenquellen abgelegten Konfiguration - in bestimmte Shards eines Datenspeichers schreibt. Es ist auch vorstellbar, dass einzelne Shards mit einem zeitlichen Verfallsdatum versehen werden. D.h. Daten werden nur auf bestimmte Zeit gespeichert.

Es ist zum vorstellbar, dass Datenquellen in dem Register festlegen, in welchen Geographien die Daten abzulegen sind (z.B. in der EU, USA, CN etc.). Das Speicherungssteuermittel kann dann so konfiguriert sein, dass es diese lnformationen aus dem Register verwendet, um die Daten nur auf Datenspeichern abzulegen, die eine validierte Lokation in der vorgegebenen Geographie aufweisen.

Gemäß einer Ausführungsform des Verfahrens gemäß der vorliegenden Anmeldung kann die Peer-to-Peer-Anwendung ein dezentrales Register, eine verteilte Ledger oder eine geteilte Datenbank sein. Das dezentrale Register kann zumindest von jedem Teilnehmer des Peer-to-Peer-Netzwerks lesbar sein. lnsbesondere können sämtliche Peer-to-Peer-Module und sämtliche Peer-Computer des Peer-to-Peer-Netzwerks vorzugsweise sämtliche lnformationen in der als Register gebildeten Peer-to-Peer-

Anwendung (oder der von der Peer-to-Peer-Anwendung kontrollierten Speicheranordnung) lesen.

Bevorzugt können auch sämtliche Peer-to-Peer-Module und sämtliche weitere Peer-Computer des Peer-to-Peer Netzwerks Nachrichten an die Peer-to-Peer-Anwendung senden oder in diese schreiben. In einfacher Weise können Informationen bevorzugt sämtlichen Teilnehmern des Peer-to-Peer Netzwerks zugänglich gemacht werden. Dies erlaubt die Durchführung einer Überprüfung der in dem dezentralen Register gespeicherten Informationen, wie ausführbare Mittel (Speicherungssteuermittel, Hashmittel etc.). Insbesondere kann vorzugsweise jeder Peer-Computer des Peer-to-Peer Netzwerks eingerichtet sein, eine Überprüfung einer neuen Information insbesondere basierend auf älteren in der Peer-to-Peer-Anwendung abgespeicherten Informationen durchzuführen.

Darüber hinaus kann gemäß einer weiteren Ausführungsform des anmeldungsgemäßen Verfahrens jeder Peer-Computer des Peer-to-Peer-Netzwerks die Peer-to-Peer-Anwendung aufweisen. Vorzugsweise kann jeder Peer-Computer, zumindest ein Teil der Peer-Computer, jeweils den kompletten Dateninhalt, zumindest jedoch einem Teil des Dateninhalts der Peer-to-Peer-Anwendung, insbesondere des dezentralen Registers, umfassen. Beispielsweise kann vorgesehen sein, dass nach einer positiven Verifizierung einer neuen in die Peer-to-Peer-Anwendung geschriebenen Information diese von sämtlichen Peer-Computern, zumindest von einem Teil der Peer-Computer, abgespeichert wird. Die Manipulationssicherheit kann hierdurch weiter verbessert werden.

Um neue Informationen manipulationssicher zu speichern, kann die Peer-to-Peer-Anwendung Verschlüsslungsmittel und/oder Signaturmittel und/oder Verifikationsmittel, beispielsweise geeignete Hash-Funktionen, umfassen. Mindestens ein Mittel der vorgenannten Mitteln kann zum Speichern von den vorgenannten Mitteln (Speicherungssteuermittel, Hashmittel etc.) eingerichtet sein. Insbesondere kann vorgesehen sein, dass durch die Hash-Funktion eine Verknüpfung mit

mindestens einer vorherigen im dezentralen Register gespeicherten lnformation hergestellt wird. Es können weitere Daten, wie Anfragen, Stamm-, Kontext- und/oder Transaktionsdaten einer Datenquelle, einer Speicheranordnung, eines Nutzers und/oder dergleichen gespeichert werden.

Bei einer besonders bevorzugten Ausführungsform kann die Peer-to-Peer Anwendung eine Blockchain oder ein dezentrale Ledger sein, umfassend mindestens zwei miteinander verknüpfte Blöcke. Die Blockchain-Technologie bzw. „decentral ledger technology" wird bereits bei der Bezahlung mittels einer Cryptowährung, wie Bitcoin, eingesetzt. Es ist erkannt worden, dass durch eine spezielle Konfiguration eine Blockchain eingerichtet werden kann, zumindest einen Bestimmungsvorgang (auch Filtervorgang genannt) für eine Bestimmung einer Speicheranordnung für einen empfangenen Datensatz manipulationssicher zu steuern.

Die Blockchain gemäß der vorliegenden Ausführungsform ist insbesondere ein dezentralisiertes, Peer-to-Peer-basiertes Register, in dem vorzugsweise eine Mehrzahl von vor genannten Mitteln (Speicherungssteuermittel, Hashmittel etc.) und Nachrichten von Datenquellen protokolliert werden können. Eine Blockchain ist als technisches Mittel besonders geeignet, eine zentrale lnstanz in einfacher und gleichzeitig sicherer Weise zu ersetzen.

Wie bereits beschrieben wurde, kann die mindestens eine Peer-to-Peer-Anwendung ein dezentralisiertes Register, ein verteiltes Ledger oder eine gemeinsam genutzte Datenbank sein, die konfiguriert ist, um Daten zu speichern, z.B. Kennung(en) oder anderen Daten, mit bestimmten Beweisen (proofs) und/oder Signaturen. Zusätzlich zu z.B. Kennung(en) von registrierten Datenquellen, kann das dezentrale Register Computercode speichern, wie z.B. ein Speicherungssteuermittel, ein Hash-Mittel, ein Überprüfungsmittel, ein Auswertemittel, ein Bewertungsmittel, ein Registriermittel etc. lnsbesondere kann der Code durch eine Transaktion an die Adresse des Codes (z.B. bei Empfang eines Datensatzes) in dem so genannten "smart contract"

aufgerufen werden. Dieser Code kann auf der Mehrzahl von Peer-Computern des Peer-to-Peer-Netzwerks (nahezu parallel) verarbeitet werden.

Es versteht sich, dass ein/e (smart contract-) Code- oder Verarbeitungslogik in sogenannten „Krypto-Bedingungen" („crypto condictions") des lnterledger-Protokolls (1LP) gespeichert und ausgeführt werden kann. Dies bedeutet, dass nicht unbedingt sämtlicher Code in einem smart contract, wie Ethereum smart contract, gespeichert sein muss.

ln einer weiteren Ausführungsform kann der (smart contract-) Code auf einem dezentralen Berechnungsmarktplatz (z. B. Ethereum Computation Market, Trubit, Golem, Cryplets Microsoft) gespeichert und ausgeführt werden.

ln einer weiteren Ausführungsform können Computercodes einer externen Rechenvorrichtung, die durch die Peer-to-Peer-Anwendung gesteuert werden, Algorithmen für dezentrale kognitive Analysen, künstliche lntelligenz oder maschinelles Lernen umfassen. Analytik und Lernen können mit anderen Geräten geteilt und über die Peer-to-Peer-Anwendung gemeinsam genutzt, aggregiert und weiter analysiert werden. Zum Beispiel können diese Algorithmen angewendet werden, um einen Auswerteschritt durchzuführen oder den Bestimmungsvorgang zu optimieren.

Ein dezentrales Register kann zumindest von einem Teil der Teilnehmer des Peer-to-Peer Netzwerks lesbar sein. lnsbesondere kann jeder Peer-Computer und jede registrierte Entität (z.B. Datenquelle, Algorithmus, Speicheranordnung etc.) (z.B. mittels des jeweiligen Peer-to-Peer-Moduls) die Peer-to-Peer Anwendung umfassen. Das dezentrale Register, zumindest der öffentliche Teil (d.h. ohne private contracts), kann zumindest von jedem Teilnehmer des Peer-to-Peer Netzwerks gelesen werden. lnsbesondere können alle Peer-to-Peer-Module und alle anderen Peer-Computer des Peer-to-Peer Netzwerks vorzugsweise sämtliche lnformationen in der Peer-to-Peer Anwendung lesen, die als Register ausgebildet ist. Vorzugsweise ist es auch möglich,

dass alle Peer-to-Peer-Module und alle anderen Peer-Computer des Peer-to-Peer-Netzwerks Nachrichten an die Peer-to-Peer Anwendung senden oder Nachrichten empfangen können.

Eine Nachricht oder Transaktion, die an einen smart contract gesendet wird, kann die Ausführung eines Codes des smart contracts (ein Speicherungssteuermittel, ein Hashmittel, ein Überprüfungsmittel, ein Auswertemittel, ein Bewertungsmittel, ein Registriermittel etc.) starten, während Daten verwendet werden, die in dem smart contract gespeichert sind. Zum Beispiel kann das Empfangen von einem Datensatz die Ausführung des mindestens einen Speicherungssteuermittels starten, wie oben beschrieben.

Die Peer-to-Peer-Anwendung kann auf folgenden Elementen aufgebaut werden: Peer-to-Peer-Netzwerk mit Consensus System/Protocol, Data Structure, Merkle Trees, Public Key Signatures und/oder Byzantinische Fehlertoleranz. Es kann Daten nach einem Consensus Prinzip replizieren. Es kann auditierbar und nachvollziehbar sein.

Auf einfache Weise können lnformationen vorzugsweise allen Teilnehmer zur Verfügung gestellt werden. Dies kann eine Überprüfung der im dezentralen Register gespeicherten lnformationen oder der im dezentralen Register ausgeführten Codes ermöglichen. Besonders bevorzugt kann jeder Peer-Computer im Peer-to-Peer-Netzwerk konfiguriert sein, um neue lnformationen zu überprüfen, insbesondere auf der Grundlage älterer lnformationen, die in der Peer-to-Peer-Anwendung gespeichert sind. Zusätzlich kann das mindestens eine Mittel (z.B. ein Speicherungssteuermittel, ein Hash-Mittel, ein Überprüfungsmittel, ein Auswertemittel, ein Bewertungsmittel, ein Registriermittel etc.) durch mindestens einen Teil der Peer-Computer des Peer-to-Peer-Netzwerks, vorzugsweise durch alle Peer-Computer, überwacht werden. Eine Manipulation eines derartigen Mittels kann somit insbesondere verhindert werden.

Darüber hinaus kann zumindest ein Peer-Computer, vorzugsweise jeder Peer-Computer, jeweils den kompletten Dateninhalt umfassen, aber zumindest einen Teil

des Dateninhalts der Peer-to-Peer-Anwendung, insbesondere des dezentralen Registers, umfassen. Beispielsweise kann vorgesehen sein, dass nach einer positiven Überprüfung einer in die Anwendung geschriebenen lnformation oder z.B. nach einer positiven Registrierung einer Datenquelle in einem Register (das von der der Peer-to-Peer-Anwendung zumindest kontrollierbar ist) diese lnformation von allen Peer-Computern, zumindest von einem Teil der Peer-Computer, gespeichert werden. Beispielsweise können nach einer erfolgreichen Registrierung einer Datenquelle die neuen Daten zumindest durch einen Teil der Peer Computer, vorzugsweise durch sämtliche Peer-Computer des Peer-to-Peer Netzwerks, gespeichert werden. Die Manipulationssicherheit für die in der Peer-to-Peer-Anwendung gespeicherten Daten kann dadurch weiter verbessert werden. Ein Bestimmungsvorgang, ein Registrierungsvorgang etc. kann sicher gesteuert werden.

Um eine neue lnformation (z.B. aus einem loT Gerät, wie einem Messgerät bzw. Sensor) in einer manipulationssicheren Weise zu speichern, kann die Peer-to-Peer-Anwendung, wie bereits beschrieben wurde, Verschlüsselungsmittel und/oder Signaturmittel und/oder Verifikationsmittel umfassen, wobei mindestens eines der Verschlüsselungsmittel und/oder der Signaturmittel und/oder Verifizierungsmittel konfiguriert ist, um Daten zu speichern. lnsbesondere kann vorgesehen sein, dass durch eine Hash-Funktion eine Verbindung mit mindestens einer zuvor gespeicherten lnformation im dezentralen Register hergestellt wird. Weitere Daten, wie z. B. Anforderungsnachrichten, gewöhnliche, kontextuelle und/oder Transaktionsdaten einer Entität können gespeichert werden. Vorzugsweise kann ein Sensor mit einer kryptographisch sicheren ldentität versehen sein. lnsbesondere werden bei dem Deployment von Code zur (direkten) Verarbeitung und / oder kryptographisch sicheren Übertagung von loT Daten Methoden des Trusted Computing verwendet (z.B. lntel SGX oder Software Secure Enclaves).

Die Peer-to-Peer Anwendung kann durch eine Directed Acyclic Graph (DAG) gebildet sein. Ein gerichteter azyklischer Graph, wie 10TA oder Tangle, bedeutet, dass Blöcke (oder Knoten des Graphen) über gerichtete Kanten miteinander gekoppelt sind. Dabei

bedeutet „direct", dass die (alle) Kanten (immer) eine gleiche Richtung in der Zeit haben. Mit anderen Worten, es ist nicht möglich, zurückzugehen. Schließlich bedeutet azyklisch, dass Schleifen nicht existieren.

ln weiteren Ausführungsformen der Peer-to-Peer-Anwendung kann die Blockchain eine „permissionless" oder „permissioned" Blockchain sein. ln einem Fall kann die Blockchain eine öffentliche, Konsortium oder private Blockchain sein.

ln einer weiteren Ausführungsform kann die Peer-to-Peer-Anwendung durch mehrere Peer-to-Peer-Netzwerke, insbesondere Blockchains, gebildet sein, die über Mechanismen wie „side chains" oder smart contracts verbunden sind. Ein Peer-to-Peer-Knoten bzw. Peer-Computer kann einen oder mehrere Blockchain-Client (s) ausführen.

Die Daten der Peer-to-Peer-Anwendung können auf der "dezentralen Ledger-Technologie" und/oder der „dezentralen Ledger-Steers (verschlüsselte) Datenspeicherung" über das lnternet und vorzugsweise in dezentralen Speicheranordnungen, Objektspeicher bzw. Datenbank gespeichert sein, wie z. B. ein lnterplanetary File System (1PFS) oder storj oder in einer verteilten Blockchain-Datenbank (z.B. BigChainDB oder mit Cryptowerk-Funktionen gehashte Datenbank). Der Zugriff auf verschlüsselte Daten an Drittanbieter kann über ein Berechtigungsmodul verwaltet werden, das als ein oder mehrere smart contract(s) in der Blockchain gebildet sein kann/können.

Wie bereits beschrieben wurde, kann vorliegend ein Mittel allgemein ein ausführbares Softwaremodul (z.B. Smart Contract) sein.

Ein weiterer Aspekt der vorliegenden Anmeldung ist ein dezentrales Speichersystem. Das dezentrale Speichersystem umfasst mindestens ein Peer-to-Peer Netzwerk mit mindestens einer Peer-to-Peer Anwendung. Die Peer-to-Peer Anwendung ist zum Empfangen mindestens eines Datensatzes, der eine Speicherungsinformation umfasst,

von einer Datenquelle eingerichtet. Die Peer-to-Peer Anwendung umfasst mindestens ein Speicherungssteuermittel. Mindestens ein Teil der Peer-Computer des Peer-to-Peer-Netzwerks ist zum Ausführen des Speicherungssteuermittels der Peer-to-Peer Anwendung eingerichtet, derart, dass basierend auf der Speicherungsinformation des Datensatzes und einem vorgegebenen Speicherungsvergleichskriteriums mindestens eine Speicheranordnung, in der der Datensatz gespeichert werden wird, aus zumindest zwei verfügbaren unterschiedlichen Speicheranordnungen durch das Speicherungssteuermittel bestimmt wird.

Das anmeldungsgemäße dezentrale Speichersystem kann insbesondere entsprechend dem zuvor beschriebenen Verfahren betrieben werden.

Ein noch weiterer Aspekt der Anmeldung ist eine Peer-to-Peer Anwendung für ein Peer-to-Peer Netzwerk (insbesondere von einem zuvor beschriebenen dezentralen Speichersystem. Die Peer-to-Peer Anwendung umfasst mindestens ein durch mindestens einem Teil der Peer-Computer des Peer-to-Peer-Netzwerks derart ausführbares Speicherungssteuermittel, dass basierend auf einer Speicherungsinformation eines empfangenen Datensatzes und basierend auf einem vorgegebenen Speicherungsvergleichskriterium mindestens eine Speicheranordnung, in der der Datensatz gespeichert werden wird, aus zumindest zwei verfügbaren Speicheranordnungen durch das Speicherungssteuermittel bestimmt wird.

Die anmeldungsgemäße Peer-to-Peer Anwendung kann insbesondere in einem zuvor beschriebenen dezentralen Speichersystem verwendet werden.

Die Merkmale der Verfahren, Systeme, Peer-to-Peer Anwendungen und Computerprogramme sind frei miteinander kombinierbar. lnsbesondere können Merkmale der Beschreibung und/oder der abhängigen Ansprüche, auch unter vollständiger oder teilweiser Umgehung von Merkmalen der unabhängigen Ansprüche, in Alleinstellung oder frei miteinander kombiniert eigenständig erfinderisch sein.

Es gibt nun eine Vielzahl von Möglichkeiten, das anmeldungsgemäße Verfahren, das anmeldungsgemäße System, und die anmeldungsgemäße Peer-to-Peer-Anwendung auszugestalten und weiterzuentwickeln. Hierzu sei einerseits verwiesen auf die den unabhängigen Patentansprüchen nachgeordneten Patentansprüche, andererseits auf die Beschreibung von Ausführungsbeispielen in Verbindung mit der Zeichnung. ln der Zeichnung zeigt:

Fig. 1 eine schematische Ansicht eines Ausführungsbeispiels eines dezentralen Speichersystems gemäß der vorliegenden Anmeldung,

Fig. 2 ein Diagramm eines Ausführungsbeispiels eines Verfahrens gemäß der vorliegenden Anmeldung,

Fig. 3 ein Diagramm eines Ausführungsbeispiels eines weiteren Verfahrens gemäß der vorliegenden Anmeldung,

Fig. 4 ein Diagramm eines Ausführungsbeispiels eines weiteren Verfahrens gemäß der vorliegenden Anmeldung,

Fig. 5 eine schematische Ansicht eines weiteren Ausführungsbeispiels eines dezentralen Speichersystems gemäß der vorliegenden Anmeldung,

Fig. 6 eine schematische Ansicht eines Ausführungsbeispiels einer Peer-to-Peer Anwendung gemäß der vorliegenden Anmeldung, und

Fig. 7 eine schematische Ansicht eines weiteren Ausführungsbeispiels eines dezentralen Speichersystems gemäß der vorliegenden Anmeldung.

ln den Figuren werden für gleiche Elemente gleiche Bezugszeichen verwendet.

Figur 1 zeigt eine schematische Ansicht eines Ausführungsbeispiels eines dezentralen Speichersystems 100 gemäß der vorliegenden Anmeldung. Das dezentrale Speichersystem 100 umfasst mindestens ein Peer-to-Peer Netzwerk 102, welches über mindestens ein Kommunikationsnetz 114 mit mindestens einer Datenquelle 110 und mindestens zwei Speicheranordnungen 120 und 122 verbunden ist. Vorzugweise werden ‚Authenticated Encryption' Verfahren oder White Box Encryption in der Kommunikation zwischen einer Datenquelle 110 und einer Speicheranordnung 120, 122 angewendet, um die Authentizität und Sicherheit der von der Datenquelle 110 an die Speicheranordnung 120, 122 kommunizierten Datensätze zu gewährleisten.

Das dezentrale Speichersystem 100 ist zum Speichern von Datensätzen 116 eingerichtet. lnsbesondere kann abhängig von einer Speichersicherheitsanforderung (z.B. ein gewünschter Speichersicherheitslevel) der empfangenen Datensätzen 116 eine Speicherung in einer Speicheranordnung 120, 122 erfolgen, die die Speichersicherheitsanforderung (z.B. das gewünschte Speichersicherheitslevel) erfüllt.

Ein wesentlicher Unterschied zu einem zentralen Speichersystem gemäß dem Stand der Technik besteht darin, dass in dem vorliegenden dezentralen Speichersystem 100 keine zentrale Steuerinstanz vorgesehen ist. Vorliegend weist das dezentrale Speichersystem 100 mindestens ein dezentrales Peer-to-Peer-Netzwerk 102 bzw. ein Rechner-Rechner-Netzwerk 102 auf. Das Peer-to-Peer-Netzwerk 102 umfasst eine Vielzahl von Peer-Computern 104.1 bis 104.3 (auch Knoten bzw. Rechner genannt). Es versteht sich, dass mehr als die dargestellten drei Peer-Computer 104.1 bis 104.3 vorgesehen sein können. Ein Peer-to-Peer-Netzwerk 102 zeichnet sich vorliegend dadurch aus, dass vorzugsweise jeder Peer-Computer 104.1 bis 104.3 und/oder Teilnehmer mit jedem anderen Peer-Computer 104.1 bis 104.3 und/oder Teilnehmer verbunden ist. Dies kann über ein drahtloses oder drahtgebundenes Kommunikationsnetz (z.B. 114) erfolgen. Beispielsweise kann das lnternet verwendet werden.

Zudem sind die Peer-Computer 104.1 bis 104.3 als gleichberechtigte Peer-Computer 104.1 bis 104.3 konfiguriert, wodurch sie sich von einer herkömmlichen Server-Client-Struktur unterscheiden.

Die dargestellten drei Peer-Computer 104.1 bis 104.3 umfassen (jeweils) eine Peer-to-Peer Anwendung 106. Wie zu erkennen ist, ist auf jedem Peer-Computer 104.1 bis 104.3 vorliegend die gleiche Peer-to-Peer Anwendung 106 implementiert. Vorzugsweise kann die Peer-to-Peer Anwendung 106 ein von insbesondere allen Teilnehmern (nicht nur den Peer-Computer 104.1 bis 104.3) des Peer-to-Peer Netzwerks 102 einsehbares öffentliches Register 106 sein. Jeder Peer-Computer 104.1 bis 104.3 weist vorzugweise das (gesamte) öffentliche Register 106 auf.

Auch kann vorgesehen sein, dass auf einem Peer-Computer nur ein Teil des Registers vorgesehen ist. ln einer besonders bevorzugten Ausgestaltung kann die Peer-to-Peer-Anwendung 106 eine Blockchain 106 sein.

Ferner ist zu erkennen, dass vorliegend der mindestens einen Datenquelle 110 (z.B. ein Gerät, Vorrichtung oder ein Teil eines Geräts/Vorrichtung, wie ein Sensor eines Geräts, ein Softwaremodul eines Geräts etc.) ein Peer-to-Peer-Modul 112 zugeordnet ist. lnsbesondere ist im vorliegenden Ausführungsbeispiel das Peer-to-Peer-Modul 112 in der Datenquelle 110 integriert.

Ein Peer-to-Peer-Modul 112 ist vorliegend insbesondere dazu eingerichtet, zumindest mit dem Peer-to-Peer-Netzwerk 102, also den Peer-Computern 104.1 bis 104.3 des Peer-to-Peer-Netzwerks 102, zu kommunizieren. Mit anderen Worten ist ein Peer-to-Peer-Modul 112 bzw. die zu diesem Peer-to-Peer-Modul 112 korrespondierende Datenquelle 110 zumindest Teilnehmer des Peer-to-Peer-Netzwerks 102. Hierbei sind jedem Teilnehmer des Peer-to-Peer-Netzwerks 102 vorzugsweise sämtliche Teilnehmer des Peer-to-Peer-Netzwerks 102 bekannt.

Vorliegend kann mittels der Peer-to-Peer-Anwendung 106 ein Bestimmungs Vorgang, von mindestens einem Teil (>1) der Peer-Computer 104.1 bis 104.3, vorzugsweise von sämtlichen Peer-Computern 104.1 bis 104.3, durchgeführt und/oder zumindest überwacht werden, wie zuvor beschrieben wurde.

Die Peer-to-Peer Anwendung umfasst mindestens ein Speicherungssteuermittel 108. Wie zu erkennen ist, ist das Speicherungssteuermittel 108 auf einer Mehrzahl von Peer-Computern 104.1 bis 104.3 implementiert. Bei einem Empfang eines Datensatzes 116, umfassend eine Speicherungsinformation 118, von einer Datenquelle 110 durch die Peer-to-Peer Anwendung 106 wird das Speicherungssteuermittel 108 auf dieser Mehrzahl von Peer-Computern 104.1 bis 104.3 gestartet und insbesondere entsprechend dem gespeicherten Computercode von diesem Teil der Peer-Computer 104.1 bis 104.3 (vorliegend sämtliche Peer-Computer 104.1 bis 104.3) ausgeführt.

Es versteht sich, dass zwei oder mehr Speicherungssteuermittel vorgesehen sein können, um eine Parallelverarbeitung von zwei oder mehr Datensätzen zu ermöglichen.

Wie bereits beschrieben wurde, sind ferner eine erste Speicheranordnung 120, die einen ersten Speichersicherheitslevel bereitstellt, und mindestens eine weitere Speicheranordnung 122, die einen weiteren Speichersicherheitslevel bereitstellt, vorgesehen. Der erste Speichersicherheitslevel unterscheidet sich insbesondere von dem mindestens einen weiteren Speichersicherheitslevel. Beispielsweise kann der erste Speichersicherheitslevel im Vergleich zum weiteren Speichersicherheitslevel höher sein. Beispielsweise kann die erste Speicheranordnung 120 als sicheres Langzeitgedächtnis und die weitere Speicheranordnung 122 als weniger sicheres Kurzzeitgedächtnis ausgebildet sein. Für eine Kommunikation zwischen dem Peer-to-Peer Netzwerk 102 und einer Speicheranordnung 120, 122 kann einer Speicheranordnung 120, 122 mindestens ein (nicht dargestelltes und zuvor beschriebenes) Peer-to-Peer Modul zugeordnet sein.

Die Funktionsweise bzw. der Betrieb des dezentralen Speichersystems 100 wird nachfolgend näher mit Hilfe der Figur 2 beschrieben. Die Figur 2 zeigt ein Diagramm eines Ausführungsbeispiels eines Verfahrens gemäß der vorliegenden Anmeldung.

ln einem ersten Schritt 201 empfängt die Peer-to-Peer Anwendung 106 einen Datensatz 116, der mindestens eine Speicherungsinformation 118 umfasst. Beispielsweise kann das Peer-to-Peer Modul (oder eine andere Komponente der Datenquelle) eingerichtet sein, einen zu sendenden Datensatz 116 mit einer Speicherungsinformation 118 zu versehen. Die Speicherungsinformation 118 umfasst insbesondere ein Speicherungskriterium, welches eine Angabe über den gewünschten Speichersicherheitslevel für den Datensatz 116 repräsentiert. ln einem einfachen Fall kann die Speicherungsinformation 118 als Speicherungskriterium ein gesetztes oder nicht gesetztes Flag sein. Anderen Codes sind möglich.

ln einem weiteren Schritt 202 (Bestimmungsvorgang) wird das Speicherungssteuermittel 108 der Peer-to-Peer Anwendung 106 durch mindestens einen Teil der Peer-Computer 104.1 bis 104.3 des Peer-to-Peer-Netzwerks 102 derart ausgeführt, dass basierend auf der Speicherungsinformation 118 des Datensatzes 116 und einem vorgegebenen Speicherungsvergleichskriteriums mindestens eine Speicheranordnung 120, 122, in der der Datensatz 116 gespeichert werden wird, aus zumindest zwei verfügbaren unterschiedlichen Speicheranordnungen 120, 122 durch das Speicherungssteuermittel 108 bestimmt wird. Das vorgegebene Speicherungsvergleichskriterium kann, bei dem oben genannten Beispiel, ein gesetztes Flag sein, das mit der ersten Speicheranordnung 120 assoziiert ist, und ein nicht gesetztes Flag, das mit der weiteren Speicheranordnung 122 assoziiert ist.

Wenn beispielsweise die Speicherungsinformation 118 als Speicherungskriterium ein gesetztes Flag umfasst, dann wird die erste Speicheranordnung 120 für die Speicherung des entsprechenden Datensatzes 116 bestimmt bzw. ausgewählt. Wenn hingegen die Speicherungsinformation 118 kein gesetztes Flag umfasst, dann wird die

weitere Speicheranordnung 122 für die Speicherung des entsprechenden Datensatzes 116 bestimmt bzw. ausgewählt.

Wie oben beschrieben wurde, sind andere Codes für die Speicherungsinformation und in entsprechender Weise für das Speicherungsvergleichskriterium möglich. ln einfacher und gleichzeitig sicherer Weise kann eine Speicheranordnung für die Speicherung eines Datensatzes bestimmt bzw. ausgewählt werden.

Die Figur 3 zeigt ein Diagramm eines weiteren Ausführungsbeispiels eines Verfahrens gemäß der vorliegenden Anmeldung. Mit Hilfe der Figur 3 wird ein weiterer beispielhafter Betrieb des dezentralen Speichersystems 100 gemäß der Figur 1 beschrieben. Es versteht sich, dass die Ausführungen auch auf andere Ausführungsbeispiele (z.B. Fig. 5) übertragen werden können. Zur Vermeidung von Wiederholungen werden nachfolgend im Wesentlichen nur die Unterschiede zu dem Ausführungsbeispiel nach Figur 2 beschrieben.

Dem nachfolgend beschriebenen beispielhaften Verfahren kann ein Registrierungsverfahren bzw. -Vorgang vorangegangen sein. lnsbesondere kann die mindestens eine Datenquelle 110 (und/oder das zugeordnete Peer-to-Peer Modul 112) in dem dezentralen Speichersystem 100, insbesondere in einem nicht dargestellten Register, registriert sein.

ln dem Registrierungsvorgang kann zumindest die eindeutige Datenquellenkennung in dem Register gespeichert werden. Wenn die Datenquelle 110 unterschiedliche Arten von Datensätze, für die unterschiedliche Speichersicherheitslevel gewünscht sind, generiert und insbesondere aussendet, kann optional zu der Datenquellenkennung für die mindestens zwei Datensatzart jeweils eine Datensatzartkennung gespeichert werden. Darüber hinaus kann in dem Registriervorgang zumindest ein Speicherungskriterium der Datenquellenkennung zugeordnet werden. Optional kann jeder Datensatzartkennung jeweils ein

Speicherungskriterium zugeordnet sein. Diese Daten können bei einer erfolgreichen Registrierung in dem Register gespeichert werden.

Der Registriervorgang kann weitere Subschritte umfassen. Bevorzugt kann die Registrierung einer Datenquelle 110 bereits während oder unmittelbar nach Herstellung der Datenquelle 110 oder während oder unmittelbar nach der lnbetriebnahme der Datenquelle 110 durchgeführt werden. Neben dem mindestens einen Kennung und des mindestens einen Speicherungskriteriums können weitere, die Datenquelle 110 betreffende Daten registriert werden („Digitales Produktgedächtnis"), wie Hersteller, Besitzer, lnstallationsort, Zustand, Daten über den Herstellungsprozess (z.B. eingesetzte Materialien, Maschinen etc.) etc.

Ein (nicht dargestelltes) Registriermittel der Peer-to-Peer Anwendung 106 kann konfiguriert sein, eine Registrierungsnachricht einer Datenquelle 110, insbesondere eines dieser Datenquelle 110 zugeordneten Peer-to-Peer-Moduls 112 zu empfangen. Die Registrierungsnachricht kann vorzugsweise zumindest die Datenquellenkennung umfassen. Das Registriermittel kann konfiguriert sein, zumindest die Datenquellenkennung in dem Register zu speichern, wie zuvor beschrieben wurde

Vor der Registrierung einer Datenquelle 110 kann zumindest ein Teil der Peer-Computer 104.1 bis 104.3 des Peer-to-Peer-Netzwerks 102, insbesondere durch eine nahezu paralleles Ausführen des Registriermittel auf jedem dieser Peer-Computer 104.1 bis 104.3, überprüfen, ob die Registrierungsanforderungen (z. B. spezifische Entitätsspezifikationen oder gültige Schlüssel oder Compliance-Anforderungen), die durch das Peer-to-Peer-Netzwerk 102 vordefiniert sind, von der Datenquelle 110, die eine Registrierung anfordert, erfüllt sind.

Alternativ oder zusätzlich kann es notwendig sein, dass eine Datenquelle 110 vordefinierte, technische Spezifikationen erfüllen muss. Um die Überprüfung durchzuführen, können vorzugsweise weitere Daten in der Registrierungsnachricht enthalten sein. lnsbesondere können die Peer-Computer 104.1 bis 104.3 des Peer-to-

Peer-Netzwerks 110 Registrierungsregeln oder Registrierungsanforderungen festlegen, die von einer Datenquelle 110 (oder einer anderen Entität (z.B. Speicheranordnung) erfüllt werden müssen, damit diese insbesondere als eine vertrauenswürdige Datenquelle 110 angesehen wird. Regeln und/oder Anforderungen können individuell von den Peer-Computern 104.1 bis 104.3 eines Peer-to-Peer-Netzwerks 102 definiert werden. Beispielsweise kann es notwendig sein, dass eine neue Datenquelle 110 oder eine neue Speicheranordnung 120, 122 von einer Entität empfohlen werden muss, die bereits Teilnehmer (Peer) des Peer-to-Peer Netzwerks 102 ist. Darüber hinaus kann es notwendig sein, dass dieser Teilnehmer einen Reputationsfaktor haben muss, der einen vordefinierten Mindestreputationsfaktor übersteigt. Bei Erfüllung des mindestens einen Kriterium kann die neue Datenquelle 110 oder die neue Speicheranordnung 120, 122 registriert werden.

ln Schritt 301 der Figur 3 wird entsprechend Schritt 201 der Figur 2 ein Datensatz 116 mit einer Speicherungsinformation 118 durch die Peer-to-Peer Anwendung 106 empfangen. Der Empfang löst insbesondere die Ausführung des Speicherungssteuermittels 108 auf dem jeweiligen Peer-Computer 104.1 bis 104.3 aus. Während der Ausführung wird insbesondere ein beispielhafter Bestimmungsvorgang 305 ausgeführt, der nachfolgend näher beschrieben wird.

Nach dem Start des Speicherungssteuermittels 108 kann zunächst in Schritt 302 die Speicherungsinformation 118 des empfangenen Datensatzes 116 ausgelesen werden. lm vorliegenden Beispiel ist die Speicherungsinformation 118 die Datenquellenkennung der aussendenden Datenquelle 110 (optional kann die Speicherungsinformation (zusätzlich) eine Datensatzartkennung umfassen). Wie bereits beschrieben wurde, wird der Schritt 302 (und auch die nachfolgend beschriebenen Schritte 303 und 304) von jedem Peer-Computer 104.1 bis 104.3, der das Speicherungssteuermittel 108 umfasst, durchgeführt.

ln einem nächsten Schritt 303 wird aus der Speicherungsinformation 118 das zugeordnete Speicherungskriterium abgeleitet bzw. bestimmt. lnsbesondere kann das Speicherungssteuermittel 108 eingerichtet sein, das zuvor beschriebene Register nach der Datenquellenkennung (und optional nach einer Datensatzartkennung) zu durchsuchen. Wird eine Korrespondenz zwischen der empfangenen Datenquellenkennung (und optional nach einer Datensatzartkennung) und einer der registrierten Datenquellenkennungen detektiert, wird das Speicherungskriterium, das der detektierten, registrierten Datenquellenkennung zugeordnet ist, ausgelesen.

ln dem nächsten Schritt 304 wird vorliegend die zu verwendende Speicheranordnung 120, 122 basierend auf dem ausgelesenen Speicherungskriterium und mindestens einem Speicherungsvergleichskriterium (zumindest implizit) bestimmt. Wenn das Speicherungskriterium beispielsweise eine Speicheranordnungskennung (1D, Adresse etc.) ist, kann der Schritt eine (implizite) Validitätsprüfung der Speicheranordnungskennung basierend auf einem entsprechenden Speicherungsvergleichskriterium in Form von validen Speicheranordnungskennung (1D, Adresse etc.) umfassen. Anschließend wird eine Weiterleitung des entsprechenden Datensatzes 116 in Schritt 306 an die bestimmte Speicheranordnung 120, 122 für eine Speicherung des Datensatzes 116 bewirkt.

Wenn das Speicherungskriterium ein gewünschter Speichersicherheitslevel ist, kann in Schritt 304 mittels eines entsprechenden Speicherungsvergleichskriterium (z.B. verschiedene Speichersicherheitslevel, die jeweils einer verfügbaren Speicheranordnung 120, 122 zugeordnet sind) geprüft werden, welche Speicheranordnung 120, 122 das gewünschte Speichersicherheitslevel erfüllt. Diese Speicheranordnung 120, 122 wird dann ausgewählt. Anschließend wird in Schritt 306 eine Weiterleitung des entsprechenden Datensatzes 116 an die bestimmte Speicheranordnung 120, 122 für eine Speicherung des Datensatzes 116 bewirkt.

Die Figur 4 zeigt ein Diagramm eines Ausführungsbeispiels eines optionalen Verfahrens gemäß der vorliegenden Anmeldung, das beispielsweise nach dem

Verfahren gemäß Figur 3 oder zumindest teilweise parallel hierzu durchgeführt werden kann.

ln Schritt 401 kann ein Bewertungsvorgang von mindestens einem gespeicherten Datensatz durchgeführt werden. Beispielsweise kann eine Mehrzahl von Datensätzen mindestens einer bestimmten Datenquelle (z.B. bestimmte Windkraftanlage, bestimmtes Fahrzeug etc.) oder einer bestimmten Datenquellen-Gruppe (z.B. bestimmte Windkraftanlagen (z.B. alle) eines bestimmten Windkraftparks, bestimmte Fahrzeuge (z.B. alle) einer bestimmten Fahrzeugflotte etc.) bewertet werden. lnsbesondere kann mindestens ein Datensatzwert und/oder ein Datenquellenwert für den mindestens einen Datensatz bestimmt werden. Beispielsweise kann als Datensatzwert und/oder ein Datenquellenwert die Zugriffszahl auf den mindestens einen gespeicherten Datensatz während einer bestimmten Zeitdauer bestimmt werden.

Dieser bestimmte Datensatzwert kann mit einem vorgegeben Vergleichswert verglichen werden (Schritt 402). Der Vergleichswert kann beispielsweise ein Grenzwert sein, der einen Bereich in zwei Teilbereiche untergliedert. Ein erster Teilbereich kann angeben, dass der Wert des mindestens einen Datensatzes derart ist, dass eine erste Speicheranordnung 120 mit einem ersten Speichersicherheitslevel verwendet werden sollte, während der zweite Teilbereich angeben kann, dass der Wert des mindestens einen Datensatzes derart ist, dass eine weitere Speicheranordnung 122 mit einem weiteren Speichersicherheitslevel verwendet werden sollte. lnsbesondere kann eine entsprechende Zugriffszahl ein lndiz für den Wert von mindestens einem Datensatz sein. Es versteht sich, dass zwei oder mehr Vergleichswerte zum Unterteilen eines Bereichs in drei oder mehr Teilbereiche (für z.B. drei oder mehr unterschiedliche Speicheranordnungen) vorgesehen sein können.

Alternativ oder zusätzlich kann das Bestimmen eines Datensatzwerts und/oder eines Datenquellenwerts das Auswerten eines Zugriffskriteriums umfassen, das für einen Zugriff auf den mindestens einen Datensatz erfüllt werden muss (Schritt 401).

Beispielsweise kann das Zugriffskriterium eine Tokenmenge (die einem bestimmten Geldwert entsprechen kann) sein, die eine weitere Entität für den Zugriff auf den mindestens einen Datensatz entrichten muss. Entsprechend den vorherigen Ausführungen kann als Vergleichswert mindestens ein Grenzwert (z.B. bestimmter Tokenwert) vorgegeben sein, mit dem der bestimmte Datensatz- und/oder Datenquellenwert verglichen werden kann (Schritt 402).

Alternativ oder zusätzlich kann das Bestimmen eines Datensatzwerts und/oder eines Datenquellenwerts das Auswerten von Sicherheitsparametern und/oder Schutzparametern des mindestens einen Datensatzes und/oder der Datenquelle des mindestens einen Datensatzes umfassen (Schritt 401). Auch dieser kann mit einem Vergleichswert anschließend verglichen werden (Schritt 402).

Es versteht sich, dass weitere Vorgaben für die Zuordnung zu einer Speicheranordnung vorgesehen sein können. Beispielsweise kann durch eine manuelle lnteraktion festgelegt sein, dass der mindestens eine Datensatz unabhängig von einem bestimmten Datensatzwert und/oder ein Datenquellenwert stets in einer bestimmten Speicheranordnung, die einen bestimmtes Speichersicherheitslevel bereitstellt, gespeichert werden muss.

lm nächsten Schritt 403 kann abhängig von dem mindestens einen Auswerte- bzw. Bewertungsergebnis, insbesondere dem mindestens einen Vergleichsergebnis, mindestens eine Handlung durch ein Bewertungsmittel einer Peer-to-Peer Anwendung initiiert werden. Beispielsweise kann basierend auf dem Ergebnis eine Änderung des Speicherungskriteriums und/oder des Speicherungsvergleichskriteriums für den mindestens einen entsprechenden Datensatz bewirkt werden. Beispielsweise kann das Speicherungskriteriums und/oder des Speicherungsvergleichskriteriums für eine bestimmte Datensatzart, eine bestimmte Datenquelle und/oder eine bestimmte Datenquellen-Gruppe geändert werden. Mit anderen Worten kann eine Rückkopplung an die Peer-to-Peer

Anwendung, an die mindestens eine Datenquelle und/oder an das Register, in dem das Speicherungskriterium gespeichert sein kann, erfolgen.

Auch kann der mindestens eine bewertete und bereits gespeicherte Datensatz in Abhängigkeit des Vergleichsergebnisses von einer ersten Speicheranordnung in eine weitere Speicheranordnung (oder umgekehrt) verschoben werden.

Optional kann das Verfahren in weiteren Schritten die gespeicherten Datensätze der mindestens einen Datenquelle/n 110 in Abhängigkeit eines Analysealgorithmus in einem Auswerteschritt auswerten. Beispielsweise kann mindestens ein neuer Datensatz basierend auf dem Auswerteergebnis generiert werden, wie zuvor beschrieben wurde.

Die Figur 5 zeigt eine schematische Ansicht eines weiteren Ausführungsbeispiels eines dezentralen Speichersystems 500, welches beispielsweise mittels der zuvor beschriebenen Verfahren betrieben werden kann. Zur Vermeidung von Wiederholungen werden nachfolgend im Wesentlichen nur die Unterschiede zu dem Ausführungsbeispiel nach Figur 1 (und den Ausführungsbeispielen nach den Figuren 2 bis 4) beschrieben. Zudem wurde zu Gunsten einer besseren Übersicht das Peer-to-Peer-Netzwerk 502 mit nur einem Peer-Computer 504 dargestellt. Es versteht sich, dass in der Regel eine Mehrzahl von Peer-Computern vorgesehen sein kann.

Vorliegend sind beispielhaft drei Datenquellen 510.1 bis 510.3 dargestellt. Die drei Datenquellen 510.1 bis 510.3 sind insbesondere Komponenten eines Systems 526, vorliegend eines Windparks 526, insbesondere Offshore-Windparks 526. Beispielhaft sind zwei Windkraftanlagen 512.1, 512.2 und eine Messboje 510.3 dargestellt. Es versteht sich, dass ein Windpark 526 eine Vielzahl weiterer Datenquellen aufweisen kann.

Für die Kommunikation mit dem Peer-to-Peer-Netzwerk 502 weist jede Datenquelle 510.1 bis 510.3 jeweils ein Peer-to-Peer Modul 512.1 bis 512.3 auf. Es versteht sich,

dass eine Datenquelle 510.1 bis 510.3 aus einer Mehrzahl von (Sub-)Datenquellen gebildet sein kann. So kann eine Windkraftanlage 510.1 bis 510.2 eine Vielzahl von Sensoren für die Messung unterschiedlichster Daten (und damit Datensatzarten) umfassen, die (Sub-) Datenquellen darstellen können. Über ein (drahtloses und/oder drahtgebundenes) Kommunikationsnetz 514 kann die Peer-to-Peer Anwendung 506 Datensätze 516 von den Datenquellen 512.1 bis 512.3 empfangen.

Die Peer-to-Peer Anwendung 506 weist vorliegend neben mindestens einem Speicherungssteuermittel 508 (z.B. inkl. einem Key Management Mittel) mindestens ein Hashmittel 528, insbesondere ein Anker-Hashmittel 528, und mindestens ein (zuvor beschriebenes) Bewertungsmittel 530 auf.

Das Anker-Hashmittel 528 ist insbesondere eingerichtet, einen empfangenen Datensatz 516 vor einer Speicherung in der bestimmten Speicheranordnung 520.1 bis 520.4 zu hashen. Vorzugsweise kann ein empfangener Datensatz 516, insbesondere dessen Roh-Daten, mit Metadaten kombiniert und der resultierende Datensatz durch das Anker-Hashmittel 528 gehasht werden, wie zuvor beschrieben wurde.

Zudem sind vorliegend vier Speicheranordnungen 520.1 bis 520.4 mit insbesondere jeweils unterschiedlichen Speichersicherheitsleveln vorgesehen. Die erste Speicheranordnung 520.1 kann beispielsweise ein 1PFS 520.1 sein, der einen ersten Speichersicherheitslevel bereitstellt, der zumindest höher ist als die Speichersicherheitslevel der weiteren Speicheranordnungen 502.2 bis 502.4. Die zweite Speicheranordnung 520.2 kann eine BigChainDB 520.2 sein, mit einem zweiten Speichersicherheitslevel, der niedriger als der Speichersicherheitslevel der ersten Speicheranordnung 520.1, aber höher als der Speichersicherheitslevel der weiteren Speicheranordnungen 520.3, 520.4 ist. Die dritte Speicheranordnung 520.3 kann eine zentrale Datenbank (z.B. von SAP) sein, mit einem dritten Speichersicherheitslevel, der niedriger als der Speichersicherheitslevel der zweiten Speicheranordnung 520.2, aber höher als der Speichersicherheitslevel der weiteren Speicheranordnung 520.4 ist. Schließlich kann als vierte Speicheranordnung 520.4 eine Cloud-

Speicheranordnung 520.4 vorgesehen sein, die in Relation zu den anderen Speicheranordnungen 520.1 bis 520.3 den niedrigsten Speichersicherheitslevel bereitstellt.

Darüber hinaus kann das dezentrale Speichersystem 500 optional mindestens eine durch die Peer-to-Peer-Anwendung 506 steuerbare (nicht gezeigte) Offchain-Rechenvorrichtung umfassen. Eine derartige Off-Chain-Rechenvorrichtung kann mindestens ein Rechenmodul beispielsweise zur Ausführung von vorgegebenen Algorithmen (z.B. umfassend kognitive Analytik, maschinelles Lernen und/oder künstlicher lntelligenz (Kl)) bereitstellen, um beispielsweise einen zuvor beschriebenen Auswerteschritt durchzuführen.

Die Figur 6 zeigt eine schematische Ansicht eines Ausführungsbeispiels einer Peer-to-Peer-Anwendung 606 gemäß der vorliegenden Anmeldung. Die Peer-to-Peer-Anwendung 606 ist insbesondere ein für die Teilnehmer eines Peer-to-Peer-Netzwerks einsehbares bzw. lesbares Register, in welches Nachrichten/Datensätze von Datenquellen, Algorithmen, Offchain-Rechenvorrichtungen, Speicheranordnungen und ähnlichen Teilnehmern des Peer-to-Peer-Netzwerks geschrieben und/oder aus dem Nachrichten/Datensätze ausgelesen werden können. Bei einem bevorzugten Ausführungsbeispiel kann die Peer-to-Peer-Anwendung 606 eine Blockchain 606 sein.

Nachfolgend wird bei der näheren Beschreibung des vorliegenden Ausführungsbeispiels davon ausgegangen, dass es sich bei der Peer-to-Peer-Anwendung 606 um eine Blockchain 606 handelt. Jedoch lassen sich die nachfolgenden Ausführungen problemlos auf andere Peer-to-Peer-Anwendungen übertragen.

Die Blockchain 606 wird aus mindestens einem Block 651 bis 655, vorzugsweise einer Vielzahl von miteinander verknüpften Blöcken 651 bis 655, gebildet. Der erste Block 651 kann auch Genesis-Block 651 genannt werden. Wie zu erkennen ist, bezieht sich ein Block 653, 655 (außer dem ersten Block 651) auf den jeweils vorherigen Block

651, 653. Ein neuer Block kann durch einen rechenintensiven Prozess (zum Beispiel so genanntes „Mining" oder durch einen entsprechenden Prozess) erschaffen werden und insbesondere allen Teilnehmern des Peer-to-Peer-Netzwerks bereitgestellt werden.

Die vorliegende Blockchain 606 ist insbesondere dazu eingerichtet Nachrichten bzw. Datensätze von einem Peer-to-Peer Modul eines Teilnehmers des Peer-to-Peer-Netzwerks, wie einem Peer-to-Peer-Modul einer zuvor beschriebenen Datenquelle, zu empfangen und diese Nachricht bzw. diesen Datensatz in der Blockchain 606 weiterzuverarbeiten. Grundsätzlich kann eine neue Nachricht in dem aktuellen Block 655 der Blockchain 614 gespeichert und veröffentlicht werden. Aufgrund der Ausgestaltung einer Blockchain 606 als öffentliches Register 606, kann die Nachricht eines Peer-to-Peer Moduls von bevorzugt sämtlichen Teilnehmern des Peer-to-Peer-Netzwerks gelesen und somit insbesondere überprüft werden. Ein zuvor beschriebener Datensatz wird jedoch - wie zuvor beschrieben wurde - in einer anderen Speicheranordnung gespeichert, dessen Zugriff durch die Blockchain 606 kontrolliert und/oder gesteuert werden kann.

ln der vorliegenden Blockchain 606 können unterschiedliche Arten von Nachrichten bzw. Datensätze, beispielsweise innerhalb eines Smart Contracts (Algorithmus und/oder Speicher auf der Blockchain) (und/oder außerhalb der Blockchain 606), verarbeitet und/oder gespeichert werden. Wie bereits beschrieben wurde, kann die Blockchain 606 ein Speicherungssteuermittel 608 umfassen. Das Speicherungssteuermittel 608 ist insbesondere ein Softwaremodul in Form eines Smart Contracts, der von dem jeweiligen Peer-Computer ausführbar ist. Die Ausführung kann insbesondere nach Erhalt eines Datensatzes gestartet und entsprechend den obigen Ausführungen durchgeführt werden. Alternativ kann ein solches Modul auch in einer vertrauenswürdige Ausführungsumgebung eingerichtet sein, die über ein Peer-to-Peer Modul an die Peer-to-Peer Anwendung angeschlossen und insbesondere von dieser steuerbar sein kann.

Neben einem Speicherungssteuermittel 608 kann die Blockchain 606 ein zuvor beschriebenes Hassmittel 628 und/oder ein zuvor beschriebenes Bewertungsmittel 630 umfassen.

Darüber hinaus ist vorliegend ein Registriermittel 634 vorgesehen. Das Registriermittel 634 ist insbesondere zum Registrieren einer Datenquelle in einem (nicht dargestellten) Register zumindest durch Speichern des der Datenquelle eindeutig zugeordneten Datenquellenkennung (und optional Datensatzartkennungen von Datensatzarten, die von dieser Datenquelle generiert werden) und mindestens einem Speicherungskriterium eingerichtet ist. Ein Registrierungsprozess kann das Durchführen eines Kommunikationstests sowie die Überprüfung weiterer, vorgebbarer Registrierungsregeln umfassen.

Ein Registrierungsprozess kann auch das Anlegen eines (dezentralen) digitalen Produktgedächtnisses bewirken. Zudem können in dem Registrierungsprozess Einzel-Komponenten einem zugehörigen System (z.B. Auto, Gebäude, Netz, Windkraftpark, Windkraftanlage etc.) zugeordnet werden (z.B. Registrierung der Komponenten in einem Konfigurationsbaum). Damit kann die ldentität einzelner Vorrichtungen/Datenquellen z.B. zu der ldentität eines Fahrzeuges, einer Windkraftanlage, eines Windkraftparks, einer Fahrzeugflotte etc. zugordnet werden.

Ferner kann eine Peer-to-Peer-Anwendung 606 grundsätzlich zur Generierung von (nicht gezeigten) Datensatzaustauschvereinbarungsmodulen eingerichtet sein. ln einem Datensatzaustauschvereinbarungsmodul bzw. -mittel kann beispielsweise festgelegt sein, welche Bedingungen für einen zulässigen Datensatzaustausch bzw. Datenzugriff eines gespeicherten Datensatzes zu erfüllen sind und zwischen welchen Entitäten (z.B. Speicheranordnung, Fahrzeug eines Nutzers, Windkraftanlage, Netzbetreiber, Versicherungsanbieter etc.) ein Austausch der Datensätze erfolgen kann.

Hierzu können die Entitäten, beispielsweise ein Peer-to-Peer-Modul einer Entität, die Generierung eines Datensatzaustauschvereinbarungsmoduls initiieren. Basierend auf den in dem Datensatzaustauschvereinbarungsmodul generierten und gespeicherten Datenelementen kann anschließend der Austauschvorgang bzw. Zugriffsvorgang durchgeführt werden. Die Generierung kann insbesondere durch Senden mindestens einer Anfragenachricht an die Peer-to-Peer-Anwendung 606 initiiert werden.

Eine Anfragenachricht kann beispielsweise Kennung/en der involvierten Entität/en, mindestens ein Zugriffskriterium, welches während oder nach dem Zugriffsvorgang erfüllt oder eingehalten werden muss, und/oder Angaben über den Dateninhalt umfassen. Es versteht sich, dass eine Anfragenachricht weniger Datenelemente oder mehr Datenelemente aufweisen kann.

Ferner kann/können mindestens ein Zugriffskriterium, vorzugsweise mehrere Zugriffskriterien, angegeben sein. Beispielsweise kann als Zugriffskriterium ein Transaktionskriterium angegeben sein. Hierbei kann es sich um ein Kriterium handeln, welches von einer Entität erfüllt werden muss, um ein Datensatzaustauschvereinbarungsmodul zu generieren. Beispielsweise kann das Transaktionskriterium eine Tokenmenge (die einem bestimmten Geldwert entsprechen kann) angeben, die eine weitere Entität für den Empfang der Daten entrichten muss.

Es versteht sich, dass andere Zugriffskriterien festgelegt sein können. Weitere Angaben können beispielsweise ein Zeitstempel, eine Kennung der Nachricht und weitere Transaktionskriterien, wie eine Angabe über die gewünschte Datenart etc., sein.

Eine weitere Nachricht kann eine Annahmenachricht sein. Die Annahmenachricht kann von einem weiteren Peer-to-Peer-Modul der weiteren Entität generiert und insbesondere an die Peer-to-Peer-Anmeldung 606 übertragen werden. Dies kann insbesondere nach einem Lesen der Anfragenachricht erfolgen.

Eine Annahmenachricht kann gleiche oder zumindest ähnliche Datenelemente wie eine zugehörige Anfragenachricht aufweisen. Zusätzlich kann die Annahmenachricht beispielsweise eine Bezugsangabe auf eine vorherige Anfrage, wie die Kennung der Anfragenachricht, umfassen.

Auch können Anfragenachrichten und/oder Annahmenachrichten direkt zwischen den Entitäten ausgetauscht werden. Vorzugsweise über ein Peer-to-Peer-Kommunikationsprotokoll.

Bei dem Zugriffskriterium kann in einer Annahmenachricht ein geringeres/höheres Transaktionskriterium angegeben sein. Falls eine Annahmenachricht ein geringeres/höheres/anderes Transaktionskriterium oder dergleichen umfasst, kann die Annahmenachricht als Gegenangebotsnachricht bezeichnet werden. Diese kann von der ersten Entität durch eine weitere Annahmenachricht angenommen werden. Basierend hierauf kann mindestens ein Peer-to-Peer-Modul die Generierung eines Datensatzaustauschvereinbarungsmoduls durch die Peer-to-Peer-Anwendung veranlassen.

lnsbesondere kann es mehrere Anfragenachrichten und/oder Annahmenachrichten geben. Jede Entität kann Vorgaben geben, nach denen mindestens ein Datensatzaustauschvereinbarungsmodul generiert werden kann. ln einem vorzugsweise automatischen, beispielsweise iterativen, Prozess kann vorzugsweise jeder Anfragenachricht eine möglichst optimal korrespondierende Annahmenachricht zugeordnet werden.

Ein (nicht gezeigtes) Datensatzaustauschvereinbarungsmodul kann innerhalb eines Smart Contracts in einem Block gespeichert sein.

Ein Smart-Contract kann vorliegend Computerprogrammcode (kurz Code) umfassen. Schließlich umfasst die Peer-to-Peer Anwendung 606 ein zuvor beschriebenes Auswertemittel 636.

lnsbesondere ist die Peer-to-Peer-Anwendung 606 dazu eingerichtet, die gespeicherten Datensätze/Nachrichten in manipulationssicherer Weise für eine Speicherung in einer durch das Speicherungssteuermittel 608 zu bestimmenden Speicheranordnung weiterzuleiten. Dies erfolgt im Wesentlichen dadurch, dass durch das gesamte Peer-to-Peer-Netzwerk zum Beispiel das Ergebnis eines Bestimmungsvorgangs von einem Speicherungssteuermittel 606 durch die kumulierte Rechenleistung des gesamten Peer-to-Peer-Netzwerks verifiziert werden kann.

Vorzugsweise können zumindest die zuvor beschriebenen Nachrichten/Datensätze in einem Block 653, 655 der Blockchain 606 durch einen Merkle-Baum paarweise miteinander gehasht werden. lnsbesondere kann nur der letzte Hashwert, der so genannte Root-Hash, als Prüfsumme in dem Header eines Blocks vermerkt werden. Dann kann der Block mit dem vorherigen Block verkettet werden. Das Verketten der Blöcke kann mithilfe dieses Root-Hashes durchgeführt werden. Jeder Block kann im Header den Hash des gesamten vorherigen Blockheaders umfassen. Dies erlaubt es, die Reihenfolge der Blöcke eindeutig festzulegen. Außerdem kann dadurch auch das nachträgliche Modifizieren vorangegangener Blöcke bzw. der in den vorherigen Blöcken gespeicherten Nachrichten (praktisch) ausgeschlossen werden, da insbesondere die Hashes aller nachfolgenden Blöcke in kurzer Zeit ebenfalls neu berechnet werden müssten.

Es versteht sich, dass die zuvor genannten Module/Datensätze etc. zumindest teilweise auch miteinander kombiniert werden können. Auch versteht es sich, dass zumindest teilweise die Daten in einer zuvor beschriebenen Speicheranordnung gespeichert werden können.

Auch kann anstelle einer linearen Blockchain ein DAG tangle oder eine Blockchain Datenbank oder ein Lightning oder State Channel Netzwerk oder eine Blockchain Integrationstechnologie, wie lnterledger Protocol oder eine Kombination der genannten Peer-to-Peer Technologien, zum Einsatz kommen.

Figur 7 zeigt eine schematische Ansicht eines weiteren Ausführungsbeispiels eines Systems 700 gemäß der vorliegenden Anmeldung. Zur Vermeidung von Wiederholungen werden nachfolgend im Wesentlichen nur die Unterschiede zu den Ausführungsbeispielen nach Figur 1 und 5 beschrieben.

Das stark vereinfacht dargestellte System 700 umfasst vorliegend sieben Entitäten 702.1, 702.2, 710.1, 710.2 die insbesondere Peer-Computer 702.1, 702.2, 710.1, 710.2 eines Peer-to-Peer-Netzwerkes 702 umfassen und/oder diese bilden. Jeder Peer-Computer 702.1, 702.2, 710.1, 710.2 kann eine (nicht dargestellte) Peer-to-Peer-Anwendung, z.B. die Blockchain 606 gemäß Figur 6, bereitstellen bzw. umfassen.

Vorliegend sind Peer-Computer 702.1, 702.2, 710.1, 710.2 durch Recheneinrichtungen 710.1, 710.2 und durch Datenquellen 702.1, 702.2, beispielsweise Sensorvorrichtungen, gebildet.

Ferner sind vorliegend insbesondere zwei unterschiedliche Arten von Peer-Computern bzw. Knotenrechnern 702.1, 710.1 bzw. 702.2, 710.2 dargestellt. Sämtliche Peer-Computer 702.1, 702.2, 710.1, 710.2 sind von dem Peer-to-Peer-Netzwerk 702 umfasst. Beim vorliegenden Ausführungsbeispiel bestimmt jedoch nur ein Teil der Peer-Computer 702.1, 702.2, 710.1, 710.2, vorliegend die Peer-Computer 702.1, 710.1 eine Speicheranordnung (oder führt eine andere Validitätsprüfung eines empfangenen Datensatzes aus) anhand der mindestens einen Speicherinformation und mindestens einem vorgegebenen Speicherungsvergleichskriteriums durch. lnsbesondere ist nur ein Teil der Peer-Computer 702.1, 710.1 eingerichtet, das (nicht gezeigte) Speicherungssteuermittel (oder ein anderes Mittel) auszuführen.

Auch kann vorgesehen sein, dass nur ein Teil der Peer-Computer die gesamte Peer-to-Peer- Anwendung speichert und/oder nur ein Teil der Peer-Computer die Algorithmen der (weiteren) Smart Contracts ausführt. Da mit der Validierung/Überprüfung ein erheblicher Rechenaufwand einhergehen kann, kann es aus Effizienzgründen von Vorteil sein, wenn nur ein Teil der Peer-Computer 702.1, 710.1, insbesondere besonders leistungsstarke Peer-Computer 702.1, 710.1, die Bestimmung der Speicheranordnungen für die empfangenen Datensätze vornehmen.

Leistungsstark meint insbesondere eine hohe Rechenleistung. Mit anderen Worten wird vorliegend von einem validen Bestimmungsergebnis einer Speicheranordnung für mindestens einen Datensatz durch die Peer-to-Peer-Anwendung, wie einer Blockchain, ausgegangen, wenn (nur) ein Teil der Peer-Computer 702.1, 710.1 zu dem gleichen Ergebnis in dem Bestimmungsvorgang gelangt ist. Es versteht sich, dass auch nur ein einzelner, insbesondere besonders leistungsstarker Peer, die Bestimmung durchführen kann. ln diesem Fall können die anderen Peer-Computer als Beobachtungs-Computer ausgeführt sein, die eingerichtet sind, zumindest die Korrektheit des Bestimmungsergebnisses zu bestätigen.

Ebenso kann bei einer alternativen (nicht gezeigten) Ausführungsform vorgesehen sein, dass ein insbesondere großes Peer-to-Peer-Netzwerk in zwei oder mehr Cluster aufgeteilt sein kann. Bei einem entsprechenden Peer-to-Peer-Netzwerk kann beispielsweise eine Validierung nur von den Mitgliedern eines Clusters durchgeführt werden.

Weiterhin kann bei einer (nicht gezeigten) Ausführungsform vorgesehen sein, dass eine Steuervorrichtung des Anbieters, Nutzers von Flottenbetreibern, Fahrzeugherstellern, Gebäudeverwaltern oder des Netzbetreibers oder zentrale Steuerungssysteme für Austauschmodulinfrastrukturen mit dem Peer-to-Peer Netzwerk verbunden sind.

lnsbesondere kann ein zuvor beschriebenes Mitel ein durch einen Peer-Computer ausführbarer Smart Contract sein.

Patentansprüche

1. Verfahren zum Betreiben eines dezentralen Speichersystems (100, 500, 700) mit mindestens einem Peer-to-Peer Netzwerk (102, 502, 702) mit mindestens einer Peer-to-Peer Anwendung (106, 506, 606), wobei das Verfahren umfasst:
   - Empfangen, durch die Peer-to-Peer Anwendung (106, 506, 606), mindestens eines Datensatzes (116, 516), der eine Speicherungsinformation (118, 518) umfasst, von einer Datenquelle (110, 510.1, 510.2, 510.3, 710), und
   - Ausführen eines Speicherungssteuermittels (108, 508, 608) der Peer-to-Peer Anwendung (106, 506, 606) durch mindestens einem Teil der Peer-Computer (104.1, 104.2, 104.3, 504, 702.1, 710.1) des Peer-to-Peer-Netzwerks (102, 502, 702), derart, dass basierend auf der Speicherungsinformation (118, 518) des Datensatzes (116, 516) und einem vorgegebenen Speicherungsvergleichskriteriums mindestens eine Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4), in der der Datensatz (116, 516) gespeichert werden wird, aus zumindest zwei verfügbaren unterschiedlichen Speicheranordnungen (120, 122, 520.1, 520.2, 520.3, 520.4) durch das Speicherungssteuermittel (108, 508, 608) bestimmt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass**
   - die empfangene Speicherungsinformation (118, 518) ein Speicherungskriterium ist oder aus der empfangenen Speicherungsinformation (118, 518) ein Speicherungskriterium bestimmbar ist, und
   - das Bestimmen der Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4) auf einem Vergleich des Speicherungskriteriums und des Speicherungsvergleichskriteriums basiert.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** mindestens ein zumindest von der Peer-to-Peer-Anwendung (106, 506, 606) kontrollierbares Hashmittel (528, 628) vorgesehen ist, und das Verfahren ferner umfasst:

- Ausführen des Hashmittels (528, 628), insbesondere durch mindestens einen Teil der Peer-Computer (104.1, 104.2, 104.3, 504, 702.1, 710.1) des Peer-to-Peer-Netzwerks (102, 502, 702), derart, dass der empfangene Datensatz (116, 516) gehasht wird, und insbesondere
- Bewirken einer Weiterleitung des gehashten Datensatzes durch das Speicherungssteuermittel (108, 508, 608) an die bestimmte Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4) für eine Speicherung des Datensatzes.

4. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass**

- die mindestens eine Datenquelle (110, 510.1, 510.2, 510.3, 710) in einem von der Peer-to-Peer Anwendung (106, 506, 606) zumindest kontrollierbaren Register registriert wird,
- wobei das Registrieren der Datenquelle (110, 510.1, 510.2, 510.3, 710) in dem Register zumindest das Speichern einer Datenquellenkennung der Datenquelle (110, 510.1, 510.2, 510.3, 710) als Speicherungsinformation (118, 518) und eines der Datenquellenkennung zugeordnetes Speicherungskriterium in dem Register umfasst.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet, dass**

- das Bestimmen der Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4) ein Bestimmen eines gespeicherten Speicherungskriterium basierend auf einem Vergleich der Speicherungsinformation (118, 518) des empfangenen Datensatzes (116, 516) mit den in dem Register gespeicherten Speicherungsinformationen umfasst, und
- das Bestimmen der Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4) auf dem bestimmten Speicherungskriterium basiert.

6. Verfahren nach Anspruch 3 und 4 oder 5, **dadurch gekennzeichnet, dass**

- das Hashmittel (528, 628) ein Anker-Hashmittel (528, 628) ist, und
- die von dem Anker-Hashmittel (528, 628) für einen von einer bestimmten Datenquelle (110, 510.1, 510.2, 510.3, 710) empfangenen Datensatzes (116, 516) erzeugten Anker-Hashwerte basierend auf einer in dem Register gespeicherten Anker-Hashspeicherungsinformation, die der Datenquellenkennung der bestimmten Datenquelle (110, 510.1, 510.2, 510.3, 710) zugeordnet ist, gespeichert werden.

7. Verfahren nach einem der vorherigen Ansprüche 2 bis 6, **dadurch gekennzeichnet, dass** das Verfahren ferner umfasst:

- Bestimmen eines Datensatzwerts und/oder eines Datenquellenwerts von mindestens einem gespeicherten Datensatz in einem Bewertungsschritt,
- Vergleichen des bestimmten Datensatzwerts und/oder Datenquellenwerts mit mindestens einem vorgegebenen Vergleichswert, und
- Bewirken einer Änderung des Speicherungskriteriums und/oder des Speicherungsvergleichskriteriums für einen entsprechenden Datensatz abhängig von dem Vergleichsergebnis.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, dass**

- der mindestens eine bewertete Datensatz abhängig von dem Vergleichsergebnis von einer ersten Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4) in eine weitere Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4) verschoben wird,
- wobei die erste Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4) in Relation zu der weiteren Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4) einen anderen Speichersicherheitslevel bereitstellt.

9. Verfahren nach Anspruch 7 oder 8, **dadurch gekennzeichnet, dass**

- das Bestimmen des Datensatzwerts und/oder des Datenquellenwerts das Bestimmen von mindestens einem gespeicherten Datensatz oder von mehreren Datensätzen einer bestimmten Datensatzart und/oder mehreren Datensätzen mindestens einer bestimmten Datenquelle (110, 510.1, 510.2, 510.3, 710) umfasst.

10. Verfahren nach einem der vorherigen Ansprüche 7 bis 9, **dadurch gekennzeichnet, dass**

- das Bestimmen des Datensatzwerts und/oder des Datenquellenwerts das Auswerten von Zugriffszahlen auf den mindestens einen Datensatz umfasst, und/oder
- das Bestimmen des Datensatzwerts und/oder Datenquellenwerts das Auswerten eines Zugriffskriteriums umfasst, das für einen Zugriff auf den mindestens einen Datensatz erfüllt werden muss, und/oder
- das Bestimmen des Datensatzwerts und/oder Datenquellenwerts das Auswerten von Sicherheitsparametern und/oder Schutzparametern des mindestens einen Datensatzes und/oder der Datenquelle (110, 510.1, 510.2, 510.3, 710) des mindestens einen Datensatzes umfasst.

11. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass**

- die gespeicherten Datensätze der mindestens einen Datenquelle/n (110, 510.1, 510.2, 510.3, 710) in Abhängigkeit eines Analysealgorithmus in einem Auswerteschritt ausgewertet werden, und
- mindestens ein neuer Datensatz basierend auf dem Auswerteergebnis generiert wird.

12. Verfahren nach Anspruch 11, **dadurch gekennzeichnet, dass**

- dem in dem Auswerteschritt verwendeten Analysealgorithmus eine Algorithmuskennung zugeordnet wird,

- wobei der Analysealgorithmus zusammen mit der Algorithmuskennung gespeichert wird, und
- wobei der erzeugte Datensatz zusammen mit der Algorithmuskennung des verwendeten Analysealgorithmus gespeichert wird.

13. Verfahren nach Anspruch 11 oder 12, **dadurch gekennzeichnet, dass**
- Datensätze von zwei oder mehr eine Gruppe bildenden Datenquellen (110, 510.1, 510.2, 510.3, 710) ausgewertet werden, und
- das Auswerteergebnis der Gruppe der Datenquellen (110, 510.1, 510.2, 510.3, 710) zugeordnet wird und zusammen mit der Gruppenkennung der Gruppe gespeichert wird.

14. Dezentrales Speichersystem (100, 500, 700), umfassend:
- mindestens ein Peer-to-Peer Netzwerk (102, 502, 702) mit mindestens einer Peer-to-Peer Anwendung (106, 506, 606),
- wobei die Peer-to-Peer Anwendung (106, 506, 606) zum Empfangen mindestens eines Datensatzes (116, 516), der eine Speicherungsinformation (118, 518) umfasst, von einer Datenquelle (110, 510.1, 510.2, 510.3, 710) eingerichtet ist, und
- wobei die Peer-to-Peer Anwendung (106, 506, 606) mindestens ein Speicherungssteuermittel (108, 508, 608) umfasst,
- wobei mindestens ein Teil der Peer-Computer (104.1, 104.2, 104.3, 504, 702.1, 710.1) des Peer-to-Peer-Netzwerks (102, 502, 702) zum Ausführen des Speicherungssteuermittels (108, 508, 608) der Peer-to-Peer Anwendung (106, 506, 606) eingerichtet ist, derart, dass basierend auf der Speicherungsinformation (118, 518) des Datensatzes (116, 516) und einem vorgegebenen Speicherungsvergleichskriteriums mindestens eine Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4), in der der Datensatz (116, 516) gespeichert werden wird, aus zumindest zwei verfügbaren unterschiedlichen Speicheranordnungen (120, 122, 520.1,

520.2, 520.3, 520.4) durch das Speicherungssteuermittel (108, 508, 608) bestimmt wird.

15. Peer-to-Peer Anwendung (106, 506, 606) für ein Peer-to-Peer Netzwerk (102, 502, 702), umfassend:

- mindestens ein durch mindestens einem Teil der Peer-Computer (104.1, 104.2, 104.3, 504, 702.1, 710.1) des Peer-to-Peer-Netzwerks () derart ausführbares Speicherungssteuermittel (108, 508, 608), dass basierend auf einer Speicherungsinformation (118, 518) eines empfangenen Datensatzes (116, 516) und basierend auf einem vorgegebenen Speicherungsvergleichskriterium mindestens eine Speicheranordnung (120, 122, 520.1, 520.2, 520.3, 520.4), in der der Datensatz (116, 516) gespeichert werden wird, aus zumindest zwei verfügbaren Speicheranordnungen (120, 122, 520.1, 520.2, 520.3, 520.4) durch das Speicherungssteuermittel (108, 508, 608) bestimmt wird.

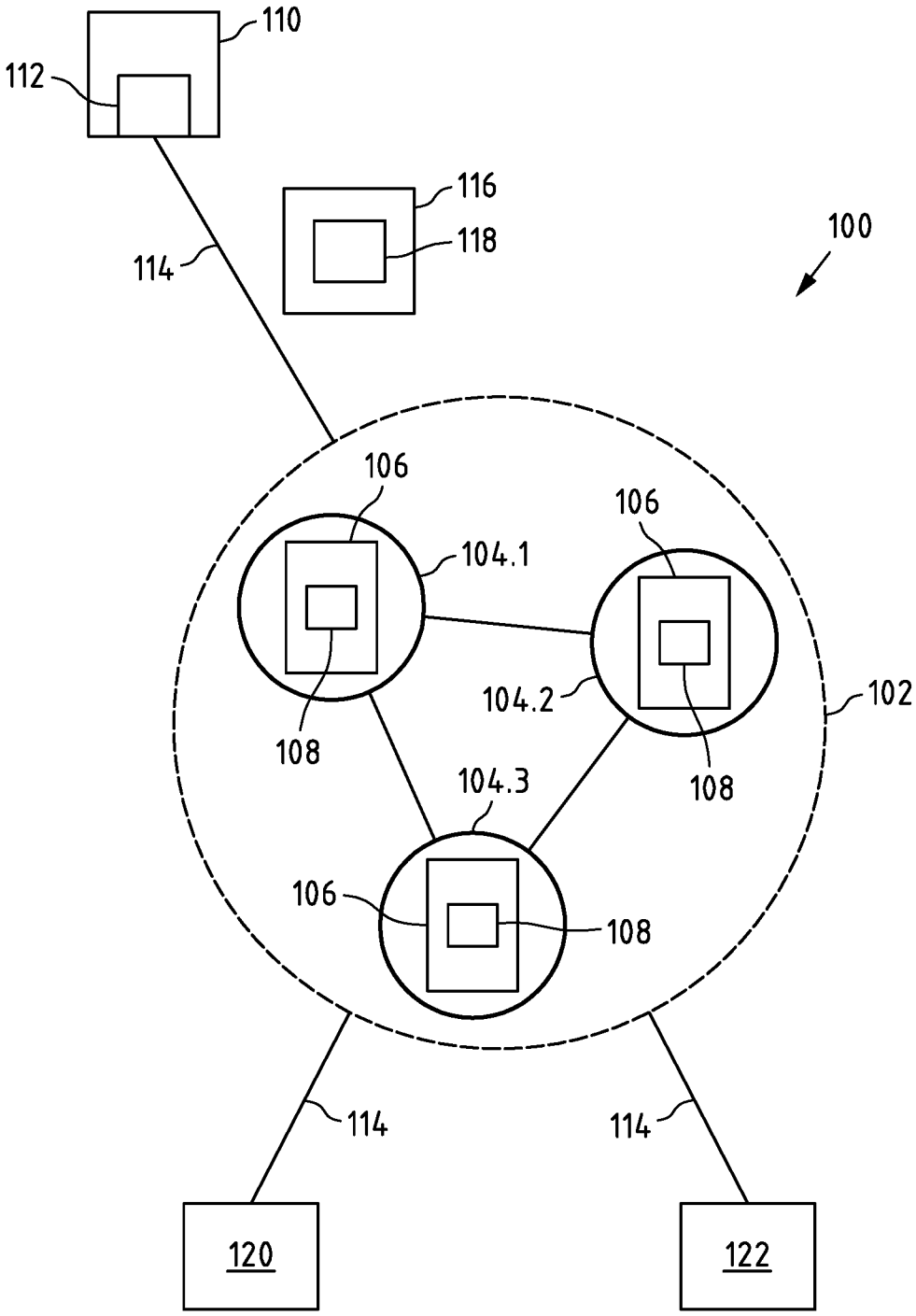
110
112
116
118
114
100
106
104.1
106
104.2
102
108
108
104.3
106
108
114
114
120
122

Fig.1

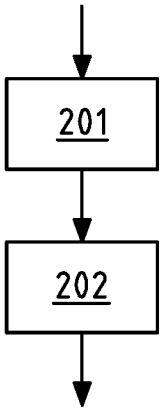

Fig.2

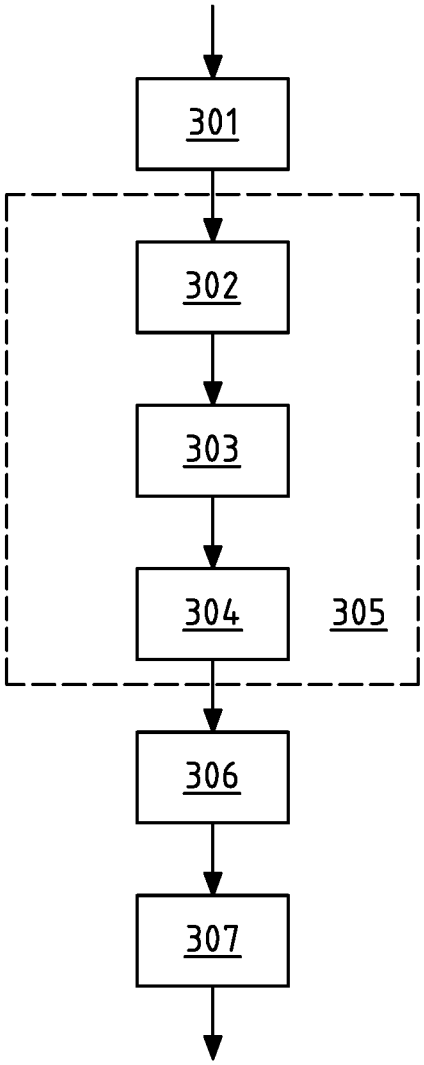

Fig.3

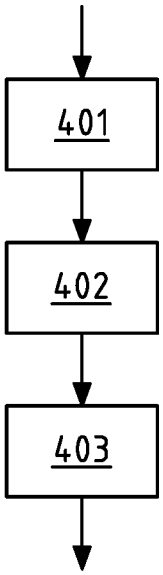

Fig.4

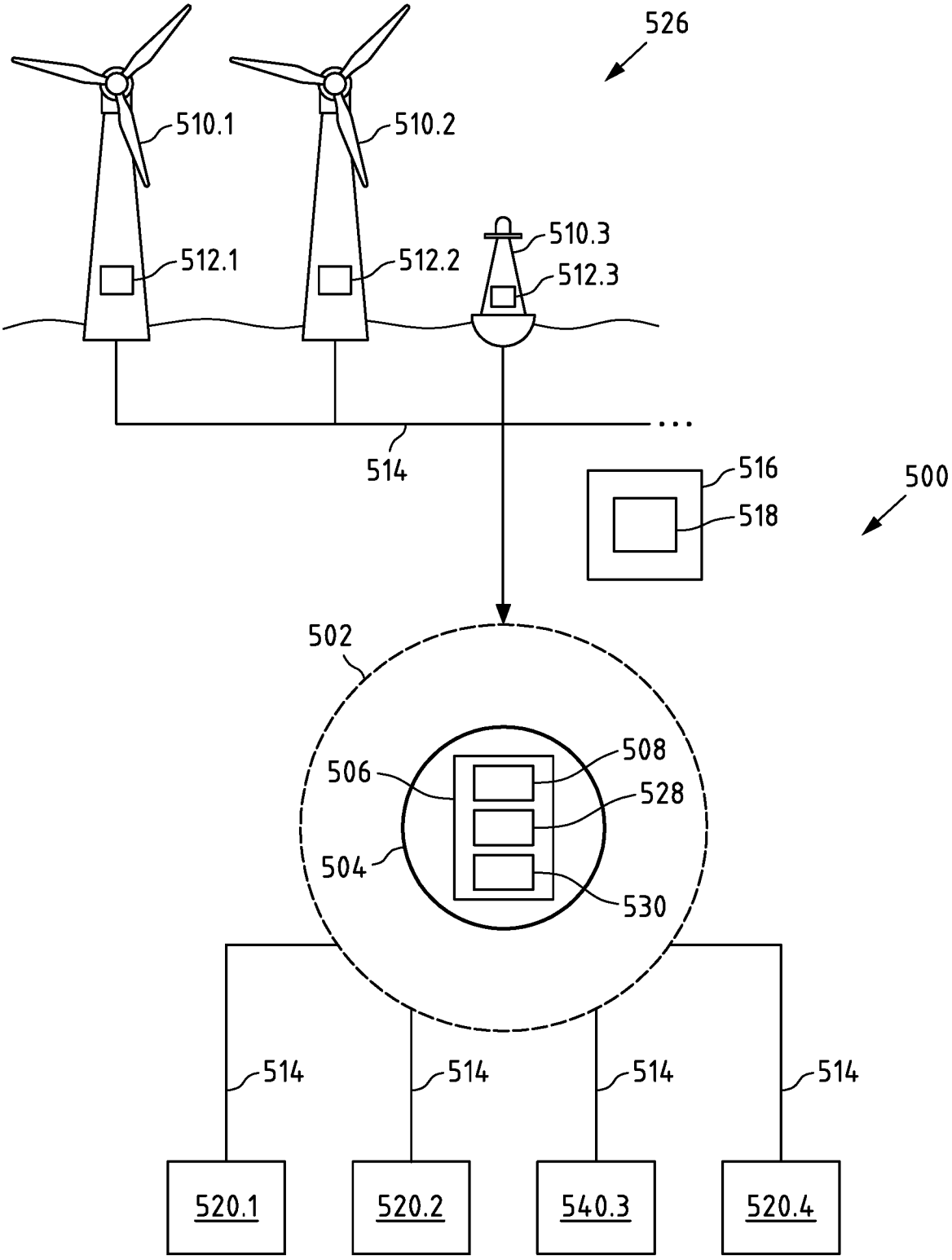
526
510.1
510.2
510.3
512.1
512.2
512.3
514
516
518
500
502
506
508
528
504
530
514
514
514
514
520.1
520.2
540.3
520.4

Fig.5

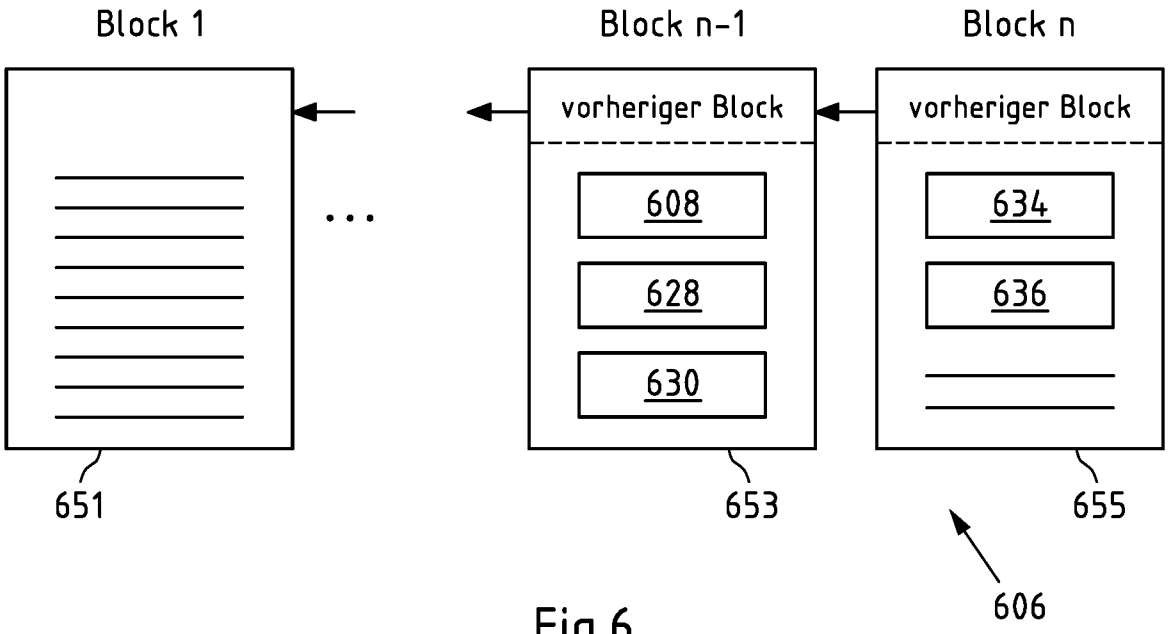
Block 1
Block n-1
Block n
vorheriger Block
vorheriger Block
608
628
630
634
636
651
653
655
606

Fig.6

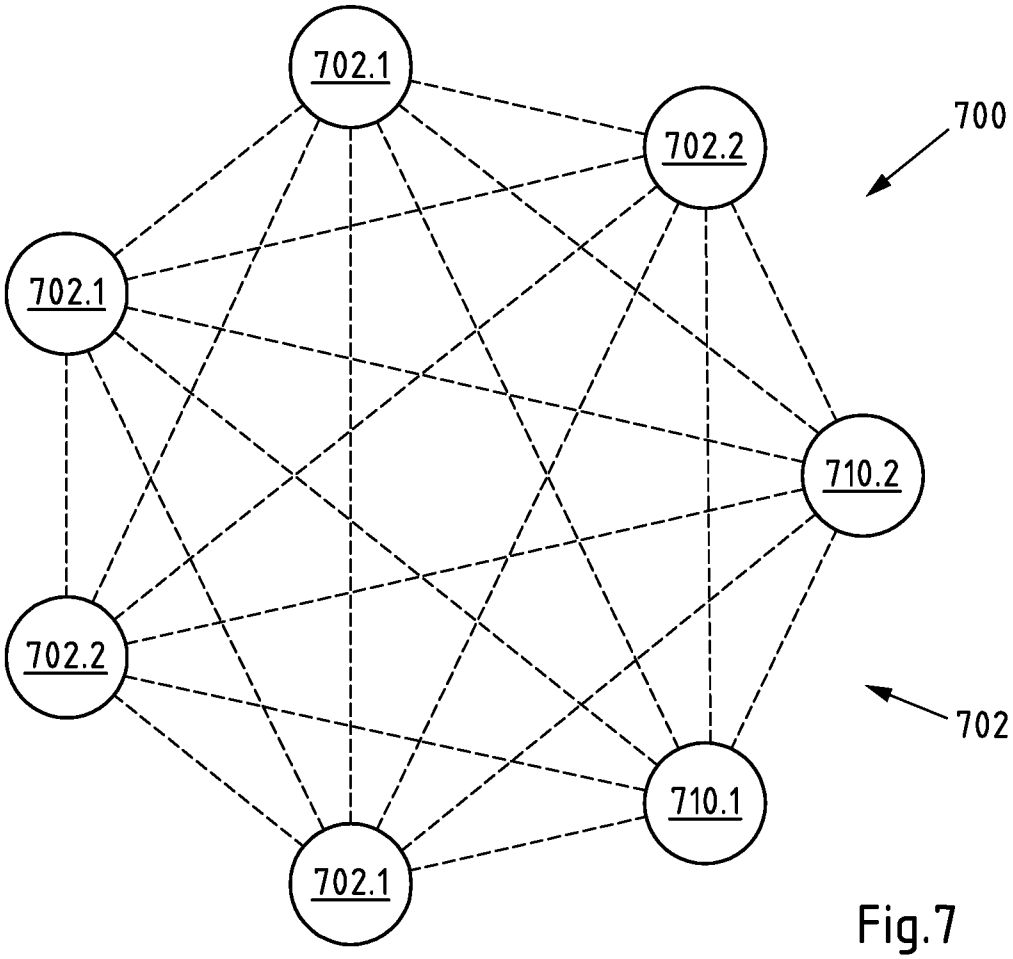
702.1
702.2
700
702.1
710.2
702.2
702
710.1
702.1

Fig.7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2018/084465

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08(2006.01)i; ***G06F 21/60***(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2017066431 A1 (TRANSACTIVE GRID INC [US]) 20 April 2017 (2017-04-20) paragraphs [0004], [0020] paragraph [0050] - paragraph [0066]	1-15
X	WO 2015057229 A1 (HEWLETT PACKARD DEVELOPMENT CO [US]) 23 April 2015 (2015-04-23) paragraph [0012] - paragraph [0021] paragraph [0034] - paragraph [0038] figures 1, 2	1-15
A	Anonymous. "Smart contract - Wikipedia" 13 December 2017 (2017-12-13), Retrieved from the Internet: https://en.wikipedia.org/w/index.php?title=Smart_contract&oldid=815244881 [retrieved on 2019-03-08] XP055566733 the whole document	1-15

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 March 2019	**15 March 2019**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Oechsner, Simon** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2018/084465

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2017066431 A1	20 April 2017	CN 108431845 A	21 August 2018
		EP 3362965 A1	22 August 2018
		US 2017103468 A1	13 April 2017
		WO 2017066431 A1	20 April 2017
WO 2015057229 A1	23 April 2015	CN 105659224 A	08 June 2016
		EP 3058490 A1	24 August 2016
		US 2016241644 A1	18 August 2016
		WO 2015057229 A1	23 April 2015

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2018/084465

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/08 G06F21/60
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L G06F

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal , WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2017/066431 A1 (TRANSACTIVE GRID INC [US]) 20. April 2017 (2017-04-20) Absätze [0004], [0020] Absatz [0050] - Absatz [0066] -----	1-15
X	WO 2015/057229 A1 (HEWLETT PACKARD DEVELOPMENT CO [US]) 23. April 2015 (2015-04-23) Absatz [0012] - Absatz [0021] Absatz [0034] - Absatz [0038] Abbildungen 1, 2 ----- -/--	1-15

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
11. März 2019	15/03/2019

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Oechsner, Simon

1

Internationales Aktenzeichen
PCT/EP2018/084465

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	Anonymous: "Smart contract - Wikipedia", , 13. Dezember 2017 (2017-12-13), XP055566733, Gefunden im Internet: URL:https://en.wikipedia.org/w/index.php?title=Smart_contract&oldid=815244881 [gefunden am 2019-03-08] das ganze Dokument -----	1-15

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2018/084465

Im Reoherohenberioht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2017066431 A l	20-04-2017	CN 108431845 A	21-08-2018
		EP 3362965 A l	22-08-2018
		US 2017103468 A l	13-04-2017
		WO 2017066431 A l	20-04-2017
WO 2015057229 A l	23-04-2015	CN 105659224 A	08-06-2016
		EP 3058490 A l	24-08-2016
		US 2016241644 A l	18-08-2016
		WO 2015057229 A l	23-04-2015